terrorisme.net

Série Mémoires et Thèses

CYBERTERRORISME, MYTHE OU RÉALITÉ ?

Cédric Thévenet

Université de Marne-La-Vallée
2005

URL: www.terrorisme.net/pdf/2006_Thevenet.pdf

Université de Marne-La-Vallée

Institut Francilien d'Ingénierie et des Services
Centre d'Etudes Scientifiques de Défense - CESD

MASTER INGENIERIE DE L'INFORMATION
DE LA DECISION ET DE LA CONNAISSANCE
Management des Risques
option Information et Sécurité

CYBER-TERRORISME, MYTHE OU REALITE ?

Cédric THEVENET

Année 2004-2005

Directeur de recherche
Amiral Pierre LACOSTE

Co-Directeur
Clément PAOLI

INTRODUCTION 5

DEFINITION DU CYBER-TERRORISME 6

LES FORMES DE L'ATTAQUE 7

1 AFFAIRE D'ETAT OU D'INDIVIDUS ? 10

1.1 LE CYBER-TERRORISME EST-IL ATTRACTIF ? 10

1.1.1 Les capacités nécessaires pour mener une attaque 10

1.1.2 Quels effets ? 11

1.1.3 Un mode d'attaque moins risqué ? 12

1.2 LES ACTEURS 12

1.2.1 Les organisations terroristes aujourd'hui 12

1.2.2 Les liens entre terroristes et pirates 13

1.2.3 les nations susceptibles de soutenir le cyber-terrorisme 14

1.3 LES NATIONS AYANT UNE POLITIQUE DE CYBER-GUERRE 16

1.3.1 La République Populaire de Chine (RPC) 16

1.3.2 Inde 16

1.3.3 Iran 17

1.3.4 Corée du Nord 18

1.3.5 Pakistan 19

1.3.6 Russie 19

1.3.7 Etats Unis d'Amérique 20

2 DE L'USAGE DU RESEAU COMME ARME 22

2.1 L'EFFET DOMINO 22

2.1.1 Impact sur les infrastructures critiques 22

2.1.2 Des interactions imprévisibles 22

2.1.3 De la vulnérabilité de certains systèmes 24

2.2 LES CLEFS DU SUCCES 24

2.2.1 La recherche de vulnérabilités par les pirates *24*

2.2.2 La rapide propagation des attaques automatisées *26*

2.2.3 La persistance des trous de sécurité *27*

2.2.4 Les erreurs de programmation *27*

2.2.5 Le risque de l'uniformité *27*

2.3 MODUS OPERANDI D'UNE INFECTION VIRALE MASSIVE **28**

2.3.1 Préambule *28*

2.3.2 Un ver particulièrement virulent *30*

2.3.3 La communication entre les vers. *32*

2.3.4 Le déni de service (DoS) *34*

2.3.5 La livraison du ver *34*

2.3.6 Une livraison ciblée *35*

2.3.7 Prise d'empreintes par pays *36*

2.3.8 L'exploitation *37*

3 ENJEUX ET RECOMMANDATIONS **38**

3.1 LES ENJEUX **38**

3.1.1 Une frappe étendue : l'exemple Black-Ice *38*

3.1.2 L'identification des cyber-terroristes *42*

3.2 RECOMMANDATIONS **43**

3.2.1 Mise en place d'une structure de réponse rapide *43*

3.2.2 Programme de réduction des menaces et vulnérabilités *46*

CONCLUSION **49**

ANNEXES **51**

A - Rapport Calipari (extrait) **51**

B - Un ver plus destructeur **54**

Bibliographie **56**

"***The FBI believes cyber-terrorism****, the use of cyber-tools to shut down, degrade, or deny critical national infrastructures, such as energy, transportation, communications, or government services, for the purpose of coercing or intimidating a government or civilian population,* ***is clearly an emerging threat for which it must develop prevention, deterrence, and response capabilities***."

Former FBI Director Lois Freeh, Statement before the United States Senate Committee on Appropriations, Armed Services, and Select Committee on Intelligence, May 10, 2001

"*It's time to work together to address the new security threats that we all face. And those threats just aren't missile, or weapons of mass destruction in the hands of untrustworthy countries.* ***Cyber-terrorism is a threat, and we need to work on that together.***"

Remarks at a joint press conference with British Prime Minister Tony Blair, july 19 2001

INTRODUCTION

Aujourd'hui, il est communément admis que les terroristes utilisent Internet pour communiquer. Ils font un usage régulier du World Wide Web pour publier des revendications, des fatwas, les vidéos d'exécution de leurs otages ou assurer leur propagande. Ils utilisent également le courrier électronique, les SMS et les téléphones satellites.

Certains pays (Sri Lanka, Indonésie, Mexique) ont reconnu avoir fait l'objet d'attaques informatiques ayant fait tomber leurs serveurs au milieu d'élections. En Europe, l'IRA a diffusé, via Internet, des informations sensibles sur les bases militaires anglaises implantées en Irlande du Nord.

Toutefois, si toutes ces actions témoignent de l'utilisation des technologies de l'information et de la communication (TIC), elles ne peuvent, pour autant, être qualifiées d'action cyber-terroriste. Identifier une action cyber-terroriste consiste à définir le terrorisme et le placer en perspective avec l'attrait que peut présenter l'utilisation des TIC.

Nous procéderons à l'évaluation de ses effets et de son attractivité puis identifierons les acteurs ou organisations susceptibles d'y avoir recours. Enfin, nous procéderons à une évaluation du risque et proposerons des recommandations visant à améliorer la sécurité de nos infrastructures sensibles.

DEFINITION DU CYBER-TERRORISME

A ce jour, il n'existe aucune définition universelle du "terrorisme". Il va donc de soit que la notion de "cyber-terrorisme" est des plus malléables. Il est également difficile, dans des délais raisonnables, de déterminer les intentions, identités ou motivations des agresseurs, qui sont des éléments nécessaire à la qualification de l'attaque.

On peut considérer que pour être qualifiée de terroriste, une action doit remplir un certain nombre de critères : l'acte doit être prémédité, motivé par des intérêts idéologiques, perpétré à l'encontre de non-combattants par des minorités nationales, ethniques, ou des agents clandestins, susceptible d'engendrer un état de panique, dans le but ultime d'influencer les gouvernants. Le terme "terrorisme international" implique des citoyens ou des territoires appartenant à plus d'un pays. Le terme "groupe terroriste" signifie, tout groupe pratiquant ou ayant un ou des sous-groupes pratiquant le terrorisme international.

Le Departement of Homeland Security (DHS) définit le cyber-terrorisme comme étant un "acte criminel perpétré au travers d'ordinateurs dont résultent des violences, décès ou destructions créant un sentiment de terreur destiné à influencer la politique d'un gouvernement"[1].

En combinant ces définitions, on peut décrire le cyber terrorisme comme étant ; une utilisation motivée par des croyances religieuses ou politiques, d'ordinateurs ou de réseaux de télécommunication, comme arme ou cible, ainsi que leur destruction physique, par des minorités ethniques, religieuses, ou des agents clandestins, dans le but d'exercer des violences à l'encontre d'une population non combattante, entraînant des pertes humaines ou des destructions, dans le but d'influencer l'opinion publique ou le gouvernement.

Cette définition est toutefois limitative car elle ne considère pas les effets secondaires d'un dysfonctionnement majeur des systèmes informatisés. On peut à titre d'exemple citer : la perte de confiance en l'économie numérique, les pertes boursières, les accidents dans les transports ou encore les problèmes d'approvisionnement d'eau et d'électricité.

[1] The truth about cyberterrorism by Scott Berinato. Definition de Ron Dick, 2002, Directeur de NIPE. <http://www.cio.com/archive/031502/truth.html>

LES FORMES DE L'ATTAQUE

Une attaque informatique peut être définie comme une action dirigée contre des systèmes informatiques dans le but de compromettre des équipements, l'exécution des processus ainsi que leur contrôle, ou de corrompre des données.

Chaque type d'attaque cible des systèmes différents ou exploitant des vulnérabilités multiples différentes et implique l'utilisation d'armes adaptées dont certaines sont aujourd'hui entre les mains de groupes terroristes.

- Une attaque physique implique des armes conventionnelles dirigées contre des centres informatiques ou des ensembles de câbles assurant les liaisons.

- Une attaque électronique implique l'utilisation de l'énergie électromagnétique comme une arme. C'est utiliser une impulsion électromagnétique pour surcharger les circuits des ordinateurs, ou, dans une forme moins violente, insérer un flux de code numérique malicieux dans les transmissions micro-onde de l'ennemi.

- Une attaque Informatique implique généralement l'utilisation de code malicieux comme arme pour infecter des ordinateurs en exploitant certaines failles logicielles. Une autre forme d'attaque informatique est l'utilisation d'informations volées pour entrer dans un système d'accès restreint.

Le Département de Défense Américain[2] a statué sur la dangerosité des différentes menaces en classant les attaques informatiques et électroniques comme étant celles présentant le plus de risques pour les Etats-Unis d'Amérique car elles peuvent provoquer des effets domino imprévisibles donnant un avantage inattendu à l'attaquant.

[2] DoD, Departement of Defense

Caractéristiques de l'attaque physique sur les réseaux informatiques

Une attaque physique interrompt la disponibilité des ordinateurs et interdit de fait l'accès aux données. Elle consiste en l'utilisation d'armes conventionnelles créant chaleur, onde de choc et/ou fragmentations dans le but de détruire physiquement les équipements.

Elle peut aussi résulter d'une utilisation directe des équipements après une pénétration dans des locaux d'accès restreint. A titre d'exemple le Pentagone a confirmé, lundi 3 mai 1999, l'utilisation par l'OTAN d'une «arme spéciale», sur laquelle il n'a donné aucune précision et qui aurait eu pour effet, dans la nuit du dimanche au lundi, puis dans la journée qui a suivi, de perturber le réseau haute tension alimentant en électricité plusieurs des grandes villes de Yougoslavie, à commencer par Belgrade. " Ce que nous avons fait, a expliqué un porte- parole, c'est de démontrer notre capacité à éteindre le système électrique quand nous le voulons, sans détruire les infrastructures de base du ravitaillement.[3] "

Caractéristiques de l'attaque électronique

Les attaques électroniques font le plus souvent référence à des impulsions électromagnétiques[4] capables d'interrompre le fonctionnement d'infrastructures informatiques en provoquant une surcharge d'énergie sur les cartes mères, transistors, et, en règle générale, tout système relié à une antenne.

Les impulsions électromagnétiques peuvent traverser les murs des locaux informatiques où elles provoquent l'effacement des mémoires, perturbent l'exécution des programmes ou endommagent définitivement les composants électroniques.

Ainsi, une attaque par impulsion électromagnétique (EMP) à haute altitude pourrait fortement perturber le fonctionnement de la société et, considérant la dépendance croissante des armées vis à vis de l'électronique, amputer gravement leurs capacités.

---

[3] Une « arme spéciale » pour couper le courant, Le Monde, 05 Mai 1999.

[4] En télécommunication, la pulsation ou impulsion électromagnétique, Electro Magnetic Pulse (EMP) en anglais désigne une émission radio brève et de très forte amplitude. La principale application est militaire : brouillage des télécommunications et destruction de matériels radios à distance. Les champs électriques et magnétiques intenses génèrent des tensions et courants destructeurs pour un appareillage radio non-protégé. La parade est l'appareil radio de quatrième génération tel le PR4G par Thomson blindé suivant le principe de la cage de Faraday contre les rayonnements électromagnétiques et à modulation par évasion de fréquence (EVF) chiffrée.

A contrario, le Ministère de l'intérieur Américain[5] déclare que les équipements civils utilisés à ce jour sont peu vulnérables et que les locaux qui hébergent les infrastructures sensibles sont bien construits et présentent des protections suffisantes.

La construction et l'utilisation d'engin EMP parait au-delà des capacités des principaux groupes terroristes. Toutefois, les nations soutenant le terrorisme ont aujourd'hui la capacité de produire un engin fonctionnel sur une portée limitée.

Caractéristiques de la cyber-attaque

Une cyber-attaque altère l'intégrité ou l'authenticité des données, habituellement au travers de l'usage de code malicieux, destiné à perturber le fonctionnement des programmes.

Les pirates informatiques[6] peuvent, à l'aide d'outils automatisés, parcourir Internet à la recherche d'ordinateurs dont les mises à jour n'ont pas été faites ou dont la configuration est défaillante afin d'en prendre le contrôle à distance. Il est également possible de faire usage de petits programmes, appelés vers[7] ou virus, qui vont se propager par leurs propres moyens et effectuer les tâches pour lesquels ils ont étés conçus.

La difficulté est de provoquer des dysfonctionnements suffisamment étendus pour qu'ils affectent directement, ou indirectement, le monde physique.

---

[5] (DHS) Departement of Homeland Security.

[6] Un « pirate informatique » désigne un individu exerçant l'une des activités (ou les deux) : - pénètre illégalement un système d'exploitation ou un serveur en cassant ses systèmes de sécurité; - copie illégalement des logiciels, en passant outre enregistrement et processus de protection. <http://www.journaldunet.com/encyclopedie/definition/223/43/20/cracker.shtml>

[7] Un ver est un programme parasite. Il n'est pas forcément auto-propageable. Son but est de grignoter des ressources système : CPU, mémoire, espace disque, bande passante... Ces petits bouts de programme sont dépendants du système d'exploitation ou d'un logiciel. Ils se propagent, comme toutes données binaires, par disquettes, CD ROM, réseaux (LAN ou WAN)... Depuis la démocratisation des virus (due notamment à la prolifération des générateurs de virus), le nombre de nouveaux vers est en net recul. Cependant, il en existe toujours. <http://www.commentcamarche.net/virus/worms.php3>

1 AFFAIRE D'ETAT OU D'INDIVIDUS ?

Considérant que les inter-connexions entre les ordinateurs pourraient multiplier les effets d'une cyber-attaque et qu'une offensive lancée sur quelques machines pourrait ensuite se propager et corrompre des milliers d'autres machines, il semblerait que le cyber terrorisme devienne, à l'avenir, une menace à considérer. Qu'en est-il aujourd'hui ?

1.1 LE CYBER-TERRORISME EST-IL ATTRACTIF ?

Il est difficile d'évaluer l'intérêt ou la capacité des groupes terroristes internationaux à lancer une attaque cyber terroriste. Certains observateurs pensent qu'Al-Qaida ne considère pas encore le cyber terrorisme comme une option susceptible de les aider à mener à bien leurs buts, l'organisation préférant les attaques physiques qui infligent dégâts matériels et pertes humaines.

Les individus susceptibles de considérer et d'employer des méthodes de cyber guerre sont originaires des sociétés post-industrielles comme les Etats-Unis d'Amérique ou l'Union Européenne, à l'inverse des groupes terroristes internationaux qui opèrent leur développement au Moyen-Orient, en Asie, en Afrique ou en Amérique du Sud (Brésil, Argentine). Toutefois, Al-Qaida a pris des mesures pour améliorer la sécurité des transmissions au sein de l'organisation au travers d'une utilisation plus intelligente des systèmes d'information. On peut donc penser que ce recours à l'informatique comme assistance à la lutte soit les prémices d'un usage plus offensif.

1.1.1 Les capacités nécessaires pour mener une attaque

La planification extensive et la surveillance pré-opérationnelle organisée par des pirates sont deux caractéristiques importantes marquant l'imminence d'une cyber-attaque. Elle consiste en la collecte de toutes les informations utiles à l'attaque et leur insertion dans une base de donnée d'où elles seront facilement extraites. Il s'agit lors de cette phase de découvrir tous les noms de domaines et de sous-domaines de l'entreprise, les types de serveurs et l'endroit où ils sont hébergés, la version des logiciels qui y sont installés, les adresses de courriel des employés, leurs numéros de téléphones, les postes qu'ils occupent, bref, obtenir une connaissance aussi exhaustive que possible de la cible.

Certains experts estiment que la planification d'une cyber-attaque, structurée et étendue, dirigée contre de multiples systèmes et réseaux, incluant la surveillance des cibles, le test de nouveaux outils, ainsi que la constitution et la formation d'une équipe prendrait entre deux et quatre ans. La planification d'une attaque massive requérant une coordination complexe, visant à causer une interruption généralisée du réseau Internet prendrait six à dix ans de préparation.

1.1.2 Quels effets ?

D'autres considèrent, comme l'a montré le cas Slammer, qu'un ver bien conçu pourrait causer d'importants dégâts sans pour autant nécessiter une préparation aussi longue.

Le ver informatique Slammer (aussi connu sous le nom de Sapphire) s'est propagé grâce à une faille sur les serveurs MS-SQL (base de données). Cette faille était employée dans les milieux warez[8] pour stocker illégalement des fichiers. Au mois de janvier 2003, Slammer s'est propagé sur Internet, ce qui a causé de graves ralentissements du réseau. Slammer a révélé que certains administrateurs réseaux n'avaient pas appliqué les correctifs nécessaires aux logiciels qu'ils utilisent. En effet, le correctif à cette faille avait été publié six mois, jour pour jour, avant la diffusion du ver.

De la même manière, le virus Tchernobyl activé lundi 26 avril 1999 pour le treizième anniversaire de la catastrophe nucléaire ukrainienne a affecté de nombreux pays d'Asie et du Moyen-orient. Il a frappé en Iran, a provoqué des dégâts en Arabie saoudite. a paralysé des dizaines d'ordinateurs en Irak. Le même virus a également frappé "sept ordinateurs" au siège de l'ONU à Bagdad[9].

On peut penser qu'un groupe terroriste pourrait hésiter à lancer une attaque terroriste, argumentant qu'il en résulterait des dommages moins immédiats et évidents, ayant donc un impact psychologiquement moindre qu'une destruction conventionnelle, comme l'explosion d'un avion, d'un bus ou d'une station de métro.

---

[8] Le terme warez est une déformation du mot anglais wares, bien qu'on y voit aussi une contraction de fantaisie de where is, qui se prononce d'ailleurs de la même façon. On nomme ainsi la mise à disposition illégale de contenus protégés, que ce soit par Internet le plus souvent mais aussi par cédérom ou toute forme de copie de fichier.

[9] Agence France Presse le 28.04.99

De même certains pensent que tant qu'une cyber-attaque ne provoquera pas de dommages physiques ou humains, elle ne sera jamais considérée comme sérieuse, tout au moins jamais aussi sérieusement qu'une attaque biologique, chimique, ou nucléaire.

1.1.3 Un mode d'attaque moins risqué ?

Le haut niveau de sécurité physique mis en place en Europe et aux Etats-Unis d'Amérique pourrait, dans le futur, inciter les terroristes à exploiter les possibilités du cyber terrorisme. En effet, les mesures de contrôle et de surveillance ainsi que les nouvelles lois anti-terroristes rendent l'action physique de plus en plus difficile à conduire. Le plan vigipirate en France rend l'accès des points sensibles plus difficile tandis que le contrôle aux frontières a été renforcé par la mise en place de passeports biométriques[10]. Ainsi, il peut paraître judicieux de planifier et de lancer une attaque depuis l'étranger sans avoir à subir les contrôles et risquer de tomber dans les filets tendus par les services de polices et de renseignements occidentaux. Ceci dit le terrorisme "traditionnel" demeure d'actualité comme en attestent les attentats de Londres de juillet dernier.

1.2 LES ACTEURS

1.2.1 Les organisations terroristes aujourd'hui

La plupart des groupes terroristes comme le Hezbollah, le Jihad Islamique ou Al-Qaida ont depuis longtemps découvert l'utilité d'Internet pour promouvoir leur cause et conduire des actions terroristes. En 2001, le site attrition.org gardait copie des sites défacés[11]. Parmi les nombreux sites touchés par des attaques de pirates, on a pu constater que nombre d'entre eux étaient des sites israéliens victimes d'organisations terroristes radicales arabes et vice versa.

Au travers de cette activité de défacement, somme toute commune aux pirates, on note que les groupes terroristes sont présents et actifs sur le réseau, qu'ils comprennent toute l'importance d'Internet et les possibilités qu'il offre dans la guerre de l'information.

---

[10] La biométrie est couramment utilisée, seule ou associée à l'anthropométrie, afin d'identifier des personnes sur la base de caractéristiques physiques individuelles. Les techniques d'identification par la biométrie servent principalement à des applications dans le domaine de la sécurité, comme le contrôle d'accès automatique, un tel dispositif étant qualifié de système de contrôle biométrique.

[11] Un défacement est un anglicisme désignant la modification non sollicitée de la présentation d'un site Web, suite au piratage de ce site. Il s'agit donc d'une forme de détournement de site Web par un pirate. Le mot anglais, qui provient de l'ancien français « desfacer », peut être rendu par « dégradation » ou « vandalisme ».

Internet permet d'engager la lutte contre l'ennemi sans perdre de précieux candidats au suicide, il permet de diffuser à volonté messages de revendications, vidéos d'exécutions[12], indications sur la fabrication de bombes, guides de fabrication de produits chimiques, etc.

Les groupes les plus marquant sur ces dernières années sont Al-Qaida muslim alliance crew, Muslim online syndicate, GForce Pakistan, PHC (Pakistan Hackers Crew).

Parmi les sites jihadistes les plus violents on note www.qalah3h.net, www.islammemo.cc ou www.alikhlas.com.

1.2.2 Les liens entre terroristes et pirates

Les liens des pirates informatiques avec des terroristes ou des nations encourageant le terrorisme sont difficiles à établir. L'adhésion à un groupe de pirates est souvent exclusive et limitée à des échanges entre les membres de l'organisation. Les outils développés sont jalousement gardés et les exploits découverts troqués en fonction des besoins. Ce type de pirate est efficace et n'attire pas l'attention, ce qui lui permet d'opérer de manière effective.

Certains groupes de pirates informatiques ont des intérêts politiques ou religieux qui dépassent le cadre national, il sont parfois qualifiés d'hacktivistes ; l'hacktivisme est une contraction de hacker et activisme qui fait référence au savoir faire technologiques et à l'analyse politique. L'hacktiviste infiltre des réseaux et met son talent au service de ses convictions politiques en organisant des attaques informatiques : piratages, détournements de serveurs, remplacement de pages d'accueil par des tracts. D'autres sont motivés par l'argent et liés à des organisations criminelles et sont prêts à vendre leurs services aux plus offrants.

Aujourd'hui, les informations portant sur les vulnérabilités des logiciels et systèmes sont à vendre sur un marché noir en ligne. On y trouve, par exemple, les adresses de 5000 ordinateurs déjà infectés et prêts à être utilisés à distance pour lancer une attaque. Le prix de vulnérabilités non publiées peut varier de 500 à 5000 dollars en fonction de leur importance. Les acheteurs de ces informations sont les compagnies spécialisées dans le spamming (envoi massif et non sollicité de courriel), les organisations criminelles et les agences gouvernementales.

---

[12] Dans une vidéo diffusée lundi 20 septembre 2004 sur un site Internet islamiste, le groupe du terroriste Al-Zarkaoui revendique l'exécution d'un otage américain, Eugene Jack Armstrong. L'homme est égorgé puis décapité.

Le Monde, Un nouvel otage est décapité, la guerre s'enfonce dans la barbarie, 20 septembre 2004

1.2.3 Les nations susceptibles de soutenir le cyber-terrorisme

Les nations soutenant le terrorisme diminuent la portée des efforts de la communauté internationale à lutter contre ce fléau. Ces états apportent une base essentielle à l'émergence d'entités organisées et efficaces. Sans le concours de ces pays, les groupes terroristes n'auraient pas, ou beaucoup plus difficilement accès aux armes, explosifs, plans et fonds nécessaires à toute action d'envergure.

L'Iran

L'Iran peut être considéré comme le pays soutenant le plus activement le terrorisme.

Au niveau institutionnel, la Garde Islamique Révolutionnaire et le Ministère de la Sécurité et du Renseignement ont été impliqués dans la planification d'actions terroristes en 2004 et encouragent le recours au terrorisme.

De plus, l'Iran reste peu disposé à juger les anciens membres d'Al-Qaida qu'il détient depuis 2003. L'identité de ces personnes est gardée secrète pour "raisons de sécurité". L'Iran a également refusé de transférer ces détenus dans leur pays d'origine ou dans un pays musulman tiers afin qu'y soient menés les interrogatoires et d'éventuelles comparutions en justice.

Par ailleurs, en 2004, l'Iran a joué un rôle non négligeable dans le conflit israelo-palestinien en encourageant les activité anti-israélienne, ceci à travers les discours de L'ayatollah Ali Khamenei[13], mais aussi grâce à des fonds et matériels à destination du Hezbollah, du HAMAS[14] ou du Front de libération de la Palestine.

La Libye

Malgré les récents accords passés entre les Etats-Unis d'Amérique, la France et l'ONU dans le but d'indemniser les victimes des attentats du vol PAN AM 103 (qui a explosé au dessus de Lockerbie en 1988) et du DC 10 d'UTA le 19 septembre 1989, la Libye reste considérée comme un état pouvant avoir recours au terrorisme.

---

[13] L'ayatollah Ali Khamenei (1939, Mechhed-) est le Guide Suprême ou Rahbar de la République islamique d'Iran. Il était l'une des principales figure lors de la révolution islamique contre le chah Mohammad Reza Pahlavi et l'un des principaux confidents de l'ayatollah Khomeini.

[14] Hamas est une abréviation pour Harakat al-Muqawama al-Islamiya (en arabe : حركة المقاومة الاسلامية « Le mouvement de résistance islamique »).

La Corée du Nord

La Corée du Nord n'est pas connue pour avoir favorisé des actions terroristes depuis l'explosion d'un avion de ligne de la Korean Airlines en 1987.

Lors d'un sommet avec le premier ministre Japonais Koizumi à Pyongyang en septembre 2002, le chef d'état, responsable de la Commission de Défense Nationale[15] Kim Jong Il, a reconnu l'implication de la Corée du Nord dans l'enlèvement de citoyens Japonais en assurant que les responsables avaient été punis.

Depuis une dizaine d'années, la Corée a adopté une stratégie militaire basée sur l'avantage asymétrique afin de compenser ses maigres ressources par des effets disproportionnés à l'investissement initial[16]. Dans ce contexte, la Corée du Nord a commencé à développer et à acquérir du matériel de haute technologie comme des missiles longue portée et pourrait avoir mené avec succès des essais nucléaires. Dans le même temps, le régime a investi dans la recherche et le développement de matériel informatique et de logiciels[17].

La Syrie

Le gouvernement syrien a continué à fournir un support politique et opérationnel au Hezbollah libanais ainsi qu'aux groupes terroristes palestiniens. Le Front Populaire de Libération de la Palestine et le jihad Islamique Palestinien, entre autres, continuent d'opérer depuis le territoire syrien. Néanmoins, la publicité de ces groupes a grandement diminué.

Les syriens ont officiellement condamné le terrorisme international mais continuent de faire une distinction entre le terrorisme et la lutte armée qu'ils considèrent légitime.

---

[15] National Defense Commission (NDC)

[16] Edward B. Atkeson et Peter Gillette, "North Korea: The Eastern End of the Access of Evil," Landpower Essay, November 2002, p. 3

[17] Alexandre Mansourov, "Bytes and Bullets: Impact of IT Revolution on War and Peace in Korea," October 2002

1.3 LES NATIONS AYANT UNE POLITIQUE DE CYBER-GUERRE

1.3.1 La République Populaire de Chine (RPC)

La RPC travaille efficacement pour atteindre le rang de grande puissance sur l'échiquier mondial. Dana ce sens, elle a déployé d'importants moyens et est parvenue à obtenir les jeux olympiques de 2008 ainsi qu'à conduire avec succès un vol dans l'espace.

Elle investit également sur des projets pharaoniques tels que la construction du barrage des trois gorges[18], un projet de pont aux dimensions inégalées, ou la construction du train le plus rapide au monde, etc.

Depuis le début des années 1990, la RPC développe ses capacités en cyber-guerre. La doctrine militaire chinoise intègre la cyber-attaque comme une composante de sa stratégie visant à défaire un ennemi mieux équipé ou supérieur en nombre.

Lors d'une allocution devant le congrès, le directeur de la CIA, George J.Tenet[19] ,a affirmé que la Chine cherchait à contourner l'avance technologique de l'armée américaine en utilisant la cyber-guerre comme arme asymétrique. La volonté de la RPC étant de faire fi de l'obsolescence de ses chars, bateaux et avions et de se concentrer sur les failles technologiques adverses. L'Armée de Libération Populaire a bien compris la dépendance sans cesse croissante des armées modernes vis à vis de l'informatique et de leur besoin permanent de communiquer.

1.3.2 Inde

Le projet de réforme de l'armée indienne datant de 1998 prévoyait qu'avant 2002 tous les officiers supérieurs devraient être formés à l'informatique. En 1999, l'Inde se dotait d'un Institut des Technologies de l'Information[20] et les premiers cours étaient donnés sur le campus temporaire de Hyderabad dans le but de former les étudiants aux rudiments de la cyber-guerre.

---

[18] Le barrage des trois gorges représente jusqu'ici le plus grand barrage, en l'occurrence le plus grand projet infra structurale dans l'histoire de l'humanité. Dans un délai de construction prévu de 17 ans, au Jangtsékiang, à proximité de la ville Yichang à la fin du fameux paysage naturel des "trois gorges" doit être établi un barrage dont la dimension n'a encore jamais été atteinte.

[19] George J. Tenet, Directeur de la CIA, Testimony Before the Senate Committee on Government Affairs, June 24, 1998.

http://www.cia.gov/cia/public_affairs/speeches/1998/dci_testimony_062498.html

[20] "Army: Now Hyper War," India Today, May 10, 1999

Dans le même temps, étaient crées trois instituts militaires délivrant un enseignement axé sur les technologies de l'information.

En 2002, est née l'Université de Défense Nationale (National Defense University) dont l'objet est la guerre de l'information et la révolution numérique. Récemment, les premier diplômés d'une licence en informatique sont sortis de cette école.

Parallèlement, l'Inde a également mis au point une stratégie de cyber-guerre incluant l'assistance du secteur privé du logiciel, si cela s'avérait nécessaire.

Le développement de moyens par le gouvernement indien s'expliquerait notamment par les activités offensives du Pakistan dans le domaine numérique. Selon Ankit Fadia, un consultant en sécurité informatique indien, les services de renseignements pakistanais paient des pirates occidentaux entre 500$ et 10.000$ pour defacer des sites Indiens. Les groupes hacktivistes défacent selon lui jusqu'à soixante sites par mois.

L'Inde s'est donné les moyens d'une réelle politique de développement informatique et a fait en sorte d'intégrer la cyber-guerre dans sa doctrine militaire. Aujourd'hui, l'Inde possède un puissant réseau de programmeurs et des centres de formation qui en font un acteur incontournable dans le monde informatique.

1.3.3 Iran

L'Iran s'ouvre aux technologies de l'information en réponse à des besoins militaires et économiques.

La tendance à la militarisation et l'isolationnisme économique pousse l'Iran à étudier avec intérêt la piste des armes non-conventionnelles, incluant une connaissance avancée des nouvelles technologies.

Certains éléments laissent à penser que la nation iranienne a commencé à développer une capacité de cyber-guerre dans le but de compenser les carences de son armée.

L'objectif de la politique iranienne est de développer le secteur des technologies de l'information tout en conservant le monopole et le contrôle des accès à Internet.

L'Iran doit gérer avec perspicacité les contradictions inhérentes à un désir de développement et d'innovation associées à une ingérence permanente de l'état.

L'accès aux sites Internet, depuis le domicile ou depuis les cyber-cafés, est limité, de par son coût financier, à une minorité aisée. Les moyens consentis par les autorités iraniennes dans le contrôle de l'Internet indiquent une maîtrise des technologies de l'information susceptible d'être utilisée dans des actions de cyber-guerre.

1.3.4 Corée du Nord

Le régime totalitaire de la Corée du Nord la dispose tout naturellement à s'intéresser de près aux technologies de l'information et de la communication.

Depuis les années 90, la Corée du Nord s'intéresse aux possibilités offertes par les nouveaux moyens de communication dans un conflit militaire.

Malgré son désir d'acquérir une capacité offensive, la Corée du Nord reste très en retrait. Ses infrastructures électroniques et industrielles sont obsolètes, les réseaux de télécommunication sont sous-dimensionnés et déficients, tout comme le réseau électrique qui souffre d'importantes faiblesses, en majeure partie à cause de son réseau sous développé.

Toutefois, le fait de placer l'armée en priorité absolue, la réelle capacité de concentration de ressources et de formation de personnel, ainsi que l'aptitude de la Corée du Nord à collecter du renseignement peuvent laisser penser que le régime a acquis la capacité de pénétrer certains réseaux et bases de données afin d'y puiser des ressources.

Le 4 Octobre 2004, le ministre de la Défense de Corée du Sud a déclaré que la Corée du Nord avait formé cinq cents pirates informatiques capables de lancer une guerre virtuelle contre les Etats-Unis d'Amérique. Selon lui, les pirates ont suivi une formation universitaire spécifique de cinq ans afin d'être capable de pénétrer les systèmes informatiques de la Corée du Sud, des Etats-Unis d'Amérique et du Japon[21].

Des rapports de renseignements ont fait état en juin et juillet 2004 d'attaques informatiques lancées contre des ordinateurs sud-coréens sensibles. Les pirates avaient infiltré deux cent onze ordinateurs de dix agences gouvernementales de Corée du Sud.

[21] Agence France Presse 04/10/2004

1.3.5 Pakistan

Le Pakistan semble concentrer ses efforts dans la préparation d'une parade aux capacités indiennes en matière de cyber-guerre. Le Pakistan présente une menace pour le réseau mondial en raison de sa population croissante de jeunes pirates informatiques. On peut constater que ceux-ci sont souvent politiquement actifs, on les trouve au coeur des conflits du monde réel. Ils sont actifs au Cachemire mais aussi en couverture sur les théâtres d'opérations impliquant des musulmans.

Il est probable qu'en réponse à l'Inde, le Pakistan étudie une manière d'exploiter plus efficacement ses ressources humaines en matière de cyber-guerre dans le but de provoquer de fortes perturbations voire un écroulement du réseau Indien.

1.3.6 Russie

La Russie, malgré son marasme économique, conserve de réelles capacités en matière d'espionnage et possède toujours d'importantes ressources, notamment en hommes.

Les capacités de cyber-guerre russes ont été mises en lumière depuis milieu des années 90 et trouvent leur illustration dans le cadre du conflit Tchétchène.

Durant le premier conflit (1994-1996), les Tchétchènes assuraient la propagande liée au conflit car le gouvernement russe taisait ses propres actions militaires permettant aux Tchétchènes de les annoncer via leurs propres canaux de communication.

Au début du second conflit (1997-2001), le gouvernement russe a compris l'intérêt de contrôler des médias et de filtrer l'information sortant de Tchétchénie.

Les Tchétchènes ont mis en place des sites hébergés en dehors de la Russie comme kavkaz.org ou qoqaz.net.my localisés en Malaisie. Sur ces sites, il était possible de télécharger des vidéos des attaques russes, de voir des photos de Tchétchénes en action. Rapidement sont apparus des sites alternatifs à www.qoqaz.net[22]. La multiplication des sites laisse apparaître une action offensive de la part de la Russie.

22 www.qoqaz.net donna naissance à plusieurs miroirs: www.qoqaz.de, www.qoqaz.com et www.qoqaz.net.my afin que lorsque l'un des miroirs était attaqué et déconnecté les autres puissent continuer à diffuser l'information.

Ainsi, en 2002, les rebelles Tchétchènes ont reconnu que deux de leurs sites, kavkaz.org et chechenpress.com, avaient été détruits par le Federalnaya Sluzhba Bezopasnosti (FSB ex-KGB). La destruction de ces sites correspond au moment de l'assaut du théâtre de Moscou par les forces spéciales le 26 Octobre 2002.

Moscou a démontré sa volonté d'utiliser toutes les armes à sa disposition, y compris la lutte informatique et a prouvé sa capacité opérationnelle.

La Russie est donc à considérer, tant par son vivier de pirates peu scrupuleux que par l'efficacité de ses services de renseignements, comme un pays possédant une réelle possibilité de nuisance sur le réseau.

1.3.7 Etats-Unis d'Amérique

En 2002, l'ancien responsable du Computer Network Attack (CNA), le Général John Bradley. disait : ''Je vous déclare que nous passons plus de temps sur les projets d'attaque informatique que sur les réseaux de défense parce que beaucoup de personnes à un niveau très élevé sont intéressées''

Pendant l'été de la même année, le président Bush signait la directive présidentielle sur la sécurité nationale n°16, ordonnant au gouvernement américain de préparer des plans nationaux de lutte électronique offensive contre des ennemis potentiels

En mars 2005, au cours d'une audience au Sénat américain, l'U.S. Strategic Command (Stratcom) révélait l'existence du Joint Functional Component Command for Network Warfare (JFCCNW).

Il s'agit d'une unité composée de hackers, au service de l'armée américaine, dont la mission prioritaire est la protection des réseaux du ministère américain de la défense, mais également une participation active au CNA.

Au cours de l'audience au sénat américain, le porte parole de Stratcom ne laissait aucun doute sur la force de frappe de l'équipe de hackers recrutés par l'armée américaine :

''Pour des raisons de sécurité, nous ne pouvons donner aucun détail. Toutefois, étant donné la dépendance de plus en plus forte aux réseaux informatiques, toute capacité informatique offensive ou défensive est grandement souhaitable".

La cyber-guerre est donc une option de la politique étrangère américaine. Toutefois deux problèmes freinent son usage :

- l'exemple récent le plus frappant des débats autour du JFCCNW concerne la diffusion sur Internet de la mort de l'otage civil américain en Irak, Nicholas Berg. Un vif conflit avait alors opposé au sein du CNA les partisans du laisser faire à ceux qui auraient souhaité que l'on détruise immédiatement le site qui diffusait la vidéo de l'exécution. Légalement, le JFCCNW ne pouvait intervenir, alors qu'une attaque par déni de service sur le site incriminé, par exemple, aurait été potentiellement réalisable. Dès la mise en ligne de la vidéo, le groupe pouvait détruire électroniquement le serveur malaysien al-ansar.net, qui hébergeait le site de diffusion de la vidéo. Mais ici, c'est la question du premier amendement de la constitution (liberté d'expression) qui se pose, et par là une censure contre le peuple américain.

- l'autre problème vient du risque de déclencher une attaque virale sans précédent sur le net. Hors, personne, pas même le JFCCNW ne peut dire quels seraient les effets d'un virus sur la globalité des réseaux mondiaux après qu'il ait accompli une mission offensive ciblée.

La directive principale reste donc, à ce jour : ''fire and forget''[23].

[23] "fait feu et oubli"

2 DE L'USAGE DU RESEAU COMME ARME

2.1 L'EFFET DOMINO

2.1.1 Impact sur les infrastructures critiques

Si beaucoup d'experts s'accordent à penser que la conjonction d'une cyber-attaque et d'une attaque conventionnelle pourrait aggraver les pertes humaines, il n'en est pas de même en ce qui concerne une attaque logique pure.

Certains pensent qu'une attaque sur les infrastructures sensibles pourrait sérieusement déstabiliser l'économie, d'autres au contraire considèrent que le réseau se remettrait en place rapidement sans trop de pertes.

Des journaux militaires Chinois ont spéculé sur le fait qu'une cyber-attaque pourrait paralyser les places boursières américaines. La Chine, étant dépendante des marchés mondiaux et notamment américains, en souffrirait également. Ainsi, la potentialité qu'un autre Etat attaque une grande nation est relativement limitée car les dégâts collatéraux sont difficilement quantifiables.

Toutefois, ce type d'attaque pourrait être mené par un groupe terroriste ou un état du tiers-monde pour qui l'économie mondiale demeure un objectif.

Dans ce contexte, en 2002, la découverte d'une faille sur le protocole de communication SNMP[24] a causé un vent de panique chez les administrateurs et responsables de réseaux. S'en est suivie une course visant à fixer le bug[25] avant qu'il soit exploité par des pirates.

2.1.2 Des interactions imprévisibles

Il est généralement admis que l'effet d'une cyber-attaque reste difficile à prévoir tant les interactions entre les systèmes sont complexes. Au contraire d'une attaque terroriste traditionnelle dont résultent des dommages immédiats, une attaque cyber-terroriste peut

[24] Le sigle SNMP signifie Simple Network Management Protocol (protocole simple de gestion de réseau en Français). Il s'agit d'un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau et de diagnostiquer les problèmes de celui-ci.

[25] Un bug, mot anglais francisé en bogue, est une anomalie de fonctionnement d'un programme informatique

impliquer un double voire un triple effet[26]. Par exemple, la libération d'un ver peut engorger des réseaux, entraînant la perte de serveurs, qui, s'ils sont importants, peuvent conduire à des ruptures d'approvisionnement en électricité, des perturbations dans les transports, etc.

- En 2003, le ver Blaster a causé une très forte perturbation des communications entre les machines connectées à Internet, ceci pendant plusieurs journées. Il semblerait qu'il ait également accentué le degré de sévérité de la rupture d'approvisionnement d'électricité en perturbant les retours d'informations entre les différents centres[27].

- Le jeudi 19 mai 2005, vers 19h15, le Samu et les sapeurs-pompiers de Paris ont été confrontés à un encombrement de lignes en raison d'un dysfonctionnement du serveur Free pendant une heure et demie. Toutes les personnes, dès lors qu'elles composaient un numéro au moyen de leur téléphone branché sur leur Freebox[28], tombaient sur le 15 ou le 18 à Paris.

- Dans un rapport confidentiel (annexe A), l'armée Américaine fait un point précis sur les circonstances qui ont mené, le 4 mars 2005, à la mort du chef de poste Italien Calipari lors de la libération de l'otage italienne Giuliana Sgrena. On y apprend que les forces qui tenaient le barrage routier n'ont pas eu connaissance de l'arrivée du convoi Italien car leur liaison Internet VoIP (Voice Over Internet Protocol) ne fonctionnait plus. C'est là un exemple concret d'effet secondaire imprévisible, causé par un dysfonctionnement informatique, ayant entraîné une perte humaine.

---

[26] Deborah P. Glass, Cyberterrorism versuses Cyberwar: at what Point does the Department of Justice turn over Cyber Incidents to the Department of Defense? (Carlisle Barracks, PA: U.S. Army War College, 2001), 5.

[27] Le ver W32.Blaster pourrait avoir contribué l'effet domino du 14 août 2003. L'impossibilité d'échanger rapidement des données entre les différents centraux électriques aurait empêché les opérateurs de contenir la propagation de la coupure de courant.

[28] La Freebox est un appareil électronique fourni par le FAI français Free à ses abonnés ADSL. Cet appareil sert principalement de modem ADSL, mais permet aussi à Free de proposer des services ajoutés utilisant le support ADSL, comme la télévision (via une prise péritel) ou la téléphonie (via une ou deux prises RJ-11 selon les modèles). Elle peut également faire office de routeur en utilisant ou non le système de transmission sans fil ASFI (traduction française du Wi-Fi).

2.1.3 De la vulnérabilité de certains systèmes

Des experts pensent que certains systèmes sont spécialement vulnérables. L'importance qu'ils jouent dans le maintien en service des infrastructures critiques en fait des cibles de choix pour les cyber-terroristes.

Les systèmes SCADA (Supervisory Control And Data Acquisition) sont des réseaux d'ordinateurs qui relient les infrastructures les plus critiques afin de surveiller leur état et de prendre automatiquement des mesures pour maintenir le bon fonctionnement de l'ensemble. Des ingénieurs accèdent ponctuellement aux systèmes SCADA pour y apporter des modifications ou effectuer des opérations de maintenance.

Selon Sharon Gaudin, expert en sécurité, la plupart des systèmes SCADA sont insuffisamment protégés contre le risque de cyber-attaque et restent vulnérables parce que les compagnies qui en ont la charge n'ont pas pris la mesure du risque et des enjeux.

D'autres experts pensent que les infrastructures sont robustes et mettraient peu de temps à se remettre d'une cyber-attaque. Ils évoquent les tempêtes qui se produisent régulièrement et qui, même si elles occasionnent des interruptions de service, ne mettent pas en danger la cohésion du réseau.

Il semble donc que pour être efficace, les cyber-terroristes devraient porter leurs attaques sur plusieurs cibles, simultanément et sur une longue période, afin de parvenir à développer un sentiment de terreur.

2.2 LES CLEFS DU SUCCES

Les ordinateurs connectés au réseau sont exposés au risque de voir certaines de leurs vulnérabilités exploitées par des pirates, par l'utilisation de vers, ou des virus, dans le but d'interrompre leur fonctionnement, d'en prendre le contrôle, ou d'en acquérir le contenu. Le nombre croissant d'ordinateurs personnels connectés à Internet avec des lignes à haut débit représente un fort potentiel d'attaque pour les pirates, pour peu qu'ils puissent les exploiter.

2.2.1 La recherche de vulnérabilités par les pirates

Les pirates utilisent aujourd'hui des automates qui balayent les plages d'adresses Internet (dites adresses IP) pour y découvrir des ordinateurs vulnérables.

L'avantage de l'automatisation du processus de découverte tient dans la constitution de bases de données contenant, pour chaque domaine ou adresse IP, la configuration de la machine, c'est à dire, son système d'exploitation[29], les services actifs et leur version.

L'automatisation permet également une temporisation du processus de prise d'empreinte qui rend sa détection par les détecteurs d'intrusions[30] (IDS) plus difficile. Le principe est ici de répartir les coups de sonde sur plusieurs jours, voire plusieurs semaines afin de les noyer dans le flux quotidien sans attirer l'attention des administrateurs.

Dès la découverte ou la publication d'une faille, les pirates disposent de listes de machines vulnérables, grâce aux bases de données où sont inscrites les adresses IP des machines scannées. Ils ont ainsi, dès la publication de la faille, un ensemble de machines vulnérables qu'ils vont pouvoir utiliser ou revendre.

Selon les observations des Computer Emergency Response Team[31] (CERT), il faut parfois plus d'un mois pour patcher la majeure partie d'un parc informatique, ce qui laisse beaucoup de temps aux pirates pour compromettre les machines de leur choix.

Les ordinateurs compromis peuvent devenir des bots, c'est à dire des machines contrôlées à distance ou semi-autonomes, capables d'infecter d'autres ordinateurs. Un individu peut alors, par ce système, contrôler simultanément des centaines voir des milliers de machines compromises.

Le pirate ayant le contrôle de ces bots, peut, à l'aide d'un tunnel chiffré, espionner les détenteurs des machines et s'approprier discrètement les données qu'elles contiennent. Il peut aussi donner l'ordre de lancer une attaque distribuée massive contre un serveur ciblé.

Même si les ordinateurs sont patchés et totalement à jour, ils ne sont pas à l'abri d'une vulnérabilité.

---

[29] Le système d'exploitation (en anglais Operating System ou OS) est chargé d'assurer la liaison entre les ressources matérielles par les pilotes et l'utilisateur par les applications (traitement de texte, jeu vidéo, etc.)

[30] Intrusion Detection System ou IDS.

[31] Les CERT (Computer Emergency Response Team) sont des centres d'alerte et de réaction aux attaques informatiques, destinés aux entreprises et/ou aux administrations, dont les informations sont généralement accessibles à tous. Le CERT conseille sur l'attitude à adopter (protections immédiates, demande d'enquête par les autorités nationales de sécurité, dépôt de plainte) et diffuse l'alerte vers d'autres organismes ou vers les CERTs étrangers, en cas d'attaque extérieure.

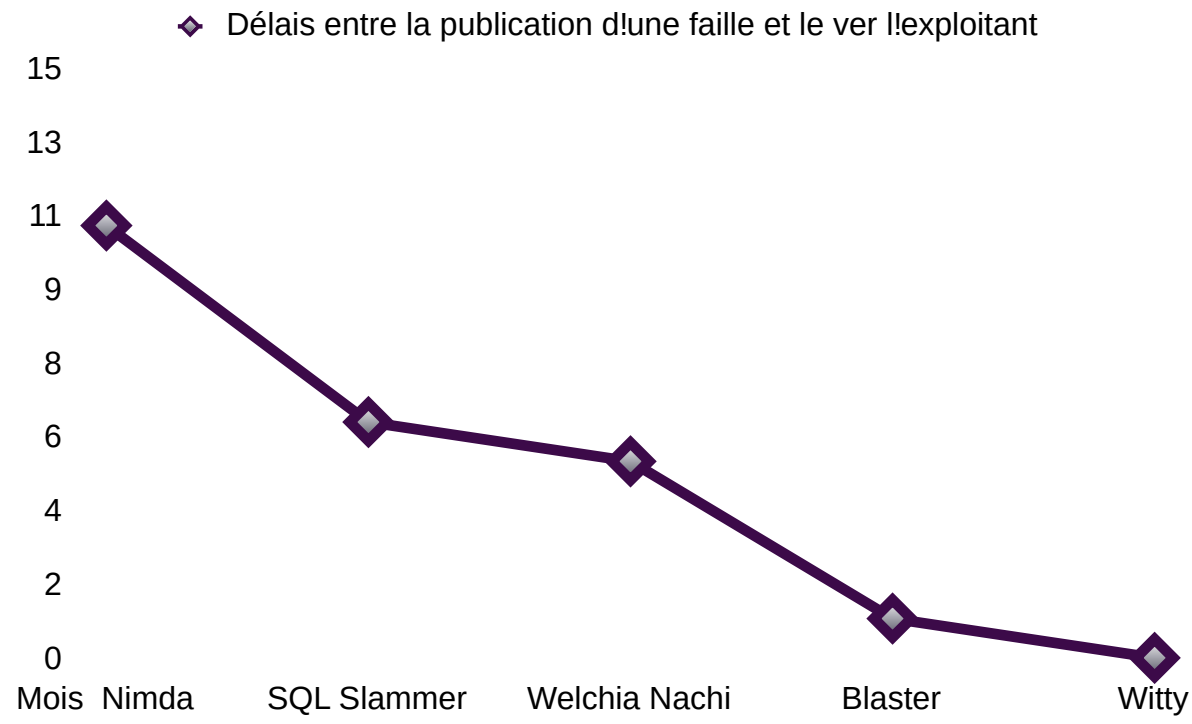
2.2.2 La rapide propagation des attaques automatisées

La vitesse de propagation des vers a fortement augmenté, passant de plusieurs jours en 2001 à trois minutes pour le ver Slammer. En janvier 2003, celui-ci a attaqué le logiciel de base de données de Microsoft et s'est répandu sur Internet en un week-end. Il a doublé la taille de l'infection toutes les dix secondes et a atteint sa pleine vitesse de scan (55 millions par seconde) après seulement trois minutes. "Slammer" a infecté 90% des ordinateurs vulnérables à travers le monde dans les dix minutes suivant sa libération, faisant de lui le ver le plus rapide de l'histoire[32].

D'après les constatations faites à l'issue de l'infection, il fut démontré que le ver exploitait une vulnérabilité pour laquelle un correctif existait depuis 2002.

Il a créé des dégâts considérables allant de l'interruption de connexion à l'annulation de vols ou de la panne de distributeurs à billet.

Le temps entre la publication d'une vulnérabilité et l'apparition d'un ver exploitant la faille en question n'a cessé de diminuer, passant de 11 mois pour Nimda à 1 jour pour Witty[33].



[32] "Internet worms keep striking" www.cbsnews.com/stories/2003/01/28/tech

[33] D'après un article de Patrick Chambet, (Edelweb), paru dans la revue "confidentiel sécurité" d'avril 2005.

2.2.3 La persistance des trous de sécurité

Les vulnérabilités dans les logiciels et la configuration des ordinateurs fournissent des points d'entrées aux pirates pour mener une cyber-attaque. Les vulnérabilités existent en grande partie grâce au manque de professionnalisme des administrateurs, à la méconnaissance des systèmes informatiques par le grand public ainsi que la très médiocre qualité des logiciels utilisés.

De plus, les utilisateurs domestiques n'ont souvent que peu, voire aucune, connaissance de la conduite à tenir en cas de risque d'infection ni les bons réflexes qui pourraient leur éviter des désagréments.

2.2.4 Les erreurs de programmation

Les vendeurs de logiciels commerciaux subissent de plus en plus de critiques parce qu'ils vendent des logiciels insuffisamment testés et porteurs d'erreurs grossières de programmation qui ouvrent la porte aux pirates. Selon Jonathan Krim du Washington Post, 80% des intrusions touchant les ordinateurs fédéraux sont attribuées à des erreurs de programmation imputables aux éditeurs.

Depuis un peu plus d'une année, Microsoft s'intéresse de plus près à la sécurité de ses produits. Il a organisé en juin 2005 la Blue Hat, conférence où il a invité des pirates pour qu'ils testent la sécurité des produits et rendent Windows moins vulnérable aux virus.

D'aprés Scott Charney, chef de la stratégie de sécurité chez Microsoft, malgré tous les efforts qui seront fait, les vulnérabilités continueront d'exister car les logiciels deviennent de plus en plus complexes et difficiles à rendre sures.

2.2.5 Le risque de l'uniformité

Le procès anti-trust lancé par plusieurs états américains à l'encontre de Microsoft a éveillé des inquiétudes quant aux risques inhérents à une monoculture logicielle.

Pour qu'une attaque informatique soit efficace, il faut qu'elle touche des ordinateurs stratégiques comme le standard d'une salle de commandement, un serveur de temps de référence, une structure de presse, le contrôle aérien ou qu'elle soit si étendue qu'elle provoque une réaction en chaîne incontrôlable affectant l'ensemble des ordinateurs sur le réseau.

Si des virus comme "Slammer" ou "Nimda"[34] ont pu provoquer une telle réaction en chaîne c'est parce que presque toutes les machines de la planète utilisaient le même système d'exploitation produit par Microsoft.

Certes un parc informatique homogène est plus facile à administrer ; les correctifs de sécurité sont les mêmes pour toutes les machines, les modifications de configurations sont valables partout et les administrateurs n'ont pas à faire l'effort de se former sur deux systèmes différents. Mais cela signifie également que tout le parc informatique est vulnérable en même temps, aux mêmes failles et que si l'on subit une attaque, il va être impossible de stopper l'infection sans déconnecter les machines et les éteindre le temps des réparations.

2.3 MODUS OPERANDI D'UNE INFECTION VIRALE MASSIVE

L'exemple suivant décrit précisément une démarche de création et de diffusion d'un ver destiné à provoquer des dysfonctionnements massifs des réseaux informationnels d'un pays. L'automatisation du processus d'attaque et sa relative simplicité de mise en place en font un exemple digne d'être explicité.

2.3.1 Préambule

Lors de la conférence BlackHat Asie 2003, l'équipe de la société Sensepost, originaire d'Afrique du Sud, a présenté une nouvelle forme d'attaque.

Considérant que la plupart des attaques via le réseau ne "font pas suffisamment mal" ils ont imaginé une approche plus subtile que les classiques dénis de service distribués[35].

Le prédicat de départ considéré par ces chercheurs est que les administrations sensibles ainsi que les grosses sociétés ne sont pas suffisamment interconnectées à Internet pour qu'une attaque venant de l'extérieur puisse les heurter au point de les paralyser.

---

[34] Nimda partage en écriture le disque de la machine infectée, se transmet aux autres ordinateurs du réseau via les dossiers partagés, sature les serveurs de mail, scanne massivement le port 80 des serveurs web et provoque des dégradations de performance voire des dénis de service.

[35] Le "Distributed denial-of-service" ou déni de service distribué est un type d'attaque très évolué visant à faire planter ou à rendre muette une machine en la submergeant de trafic inutile. Plusieurs machines à la fois sont à l'origine de cette attaque (c'est une attaque distribuée) qui vise à anéantir des serveurs, des sous-réseaux, etc. D'autre part, elle reste très difficile à contrer ou à éviter. C'est pour cela que cette attaque représente une réelle menace. <http://www.securiteinfo.com/attaques/hacking/ddos.shtml>

Forts de cette réflexion, ils se sont interrogés sur leurs besoins pour mener à bien leur projet. Leur réponse a été : Nous avons besoin d'attaques ciblées, effectives et automatisées, suffisamment coordonnées et étendues pour paralyser un pays.

L'outil le plus approprié est apparu comme étant un ver[36].

Cela fait déjà longtemps que la pertinence des attaques depuis Internet est débattue. Si l'on devait les scinder en deux groupes, on placerait d'un coté les attaques par DDoS et de l'autre les intrusions[37]. Ces deux méthodes semblent inefficaces pour paralyser un pays.

Si un déni de service est déplaisant, il est largement inefficace contre les réseaux internes des sociétés et des administrations visées. Pour les organismes non intensivement reliés à Internet (ex: militaires), ce type d'attaques ne pose pas de réel problème car elles peuvent couper leur connexion sans affecter leurs organes de commandement et d'information.

Le second type d'attaque, le "hacking in", pose un gros problème pour tout organisme publique ou privé, mais à l'échelle d'un pays il est difficile d'imaginer que suffisamment d'unités, dans le même secteur, soient touchées de manière simultanée. Même avec la découverte d'un 0day[38] les pirates n'auraient pas une connaissance suffisante de la cible à laquelle ils s'attaquent.

La création d'un ver utilisant un 0day virulent capable de toucher simultanément tous les domaines spécifiques d'un pays devient, à la lumière de cette réflexion, un concept très intéressant. On considère qu'il existe aujourd'hui une vingtaine de « bons » 0days en circulation dans les milieux alternatifs, d'une valeur financière tournant autour de 3000 dollars et pouvant atteindre beaucoup plus. Le temps de recherche est d'environ une dizaine de jours pour trouver une faille exploitable dans Windows XP SP2.

---

[36] voir note de bas de page numéro 7.

[37] L'intrusion, ou hacking in: terme désignant les méthodes (légales ou non) visant à "casser" des protections (dès qu'une protection a été cassé ou est susceptible d'être cassé...on parle alors de faille).

[38] Un 0day (zéro jour) est une vulnérabilité pour laquelle il n'existe pas de correctif. Kostya Kortchinsky, responsable du CERT RENATER, "0day" SSTIC '05 à Rennes.

2.3.2 Un ver particulièrement virulent

Il est généralement entendu que les vers peuvent être beaucoup plus évolués que leurs manifestations habituelles. Ils apparaissent généralement quelques semaines ou mois après qu'une vulnérabilité ait été découverte. Les programmes malicieux associent, à l'exploit qui utilise la vulnérabilité, un moyen de propagation.

Le ver, ainsi constitué, se répand sur la toile, libre et sans contrôle, rapidement dans un premier temps puis plus lentement au fil des jours et semaines au rythme des patches appliqués et anti-virus mis à jour.

Certains vers ont la capacité de cibler le réseau interne et d'y créer de fortes perturbations même s'ils n'ont pas été conçus dans le but de créer un déni de service.

Les administrateurs se précipitant pour appliquer les patches logiciels aux serveurs affectés font habituellement du bon travail en désinfectant leur propre parcelle du parc informatique de leur employeur. Sitôt l'infection contenue et les machines patchées, les administrateurs se tournent souvent trop rapidement vers d'autres tâches, de nombreux problèmes se posant à eux pour maintenir le parc informatique à jour :

- Nouveaux serveurs ajoutés,

- Serveurs réinstallés avec les solutions logicielles obsolètes,

- Les branches du réseau non-affectées restent souvent vulnérables,

- La plupart des vers exploitent une vulnérabilité spécifique ; les administrateurs tendent à se concentrer sur ce problème particulier en occultant les autres.

- Les administrateurs ont tendance à utiliser leurs ressources humaines et financières à construire une "barrière forte" sous forme d'antivirus et à scanner le contenu plutôt que de garder les vers dehors et de patcher toutes les machines internes.

- La plupart des vulnérabilités à l'intérieur des réseaux locaux peuvent être attribuées à des "grosses négligences" et des erreurs de configuration plutôt qu'à des vulnérabilités spécifiques.

On constate aujourd'hui que l'industrie de la sécurité s'est orientée vers la création d'un périmètre destiné à devenir infranchissable. On peut comparer ce concept à un igloo, dur à l'extérieur et tendre à l'intérieur. Dans toutes ces évaluations l'équipe Sensepost a trouvé, à un degré ou à un autre, au sein des intranets, des vulnérabilités qui auraient du être corrigées et qui ne demandaient qu'à être exploitées[39]. Beaucoup de ces vulnérabilités existaient depuis longtemps, mais il y a très peu d'administrateurs en charge du management de réseaux étendu qui pourraient honnêtement prétendre qu'aucune d'entre elles n'est présente sur leur parc. Pourtant toutes ces vulnérabilités permettent une prise de commande à distance.

Nombreux sont ceux qui s'accordent à dire qu'un ver exploitant un 0day, lancé sur des réseaux internes, pourrait infecter un grand nombre de machines. Combiné avec un déni de service, un tel ver pourrait paralyser jusqu'aux plus grands des réseaux locaux[40].

Quand on crée un ver qui doit opérer exclusivement sur un réseau local, on doit garder à l'esprit un certain nombre de règles:

- Le ciblage de nouvelles victimes est sensiblement différent des vers basés sur Internet.

- Le ver va se propager à la vitesse maximale permise par l'infrastructure physique du réseau local. La propagation par elle-même pourrait causer un DDoS.

- La composante du DoS de tous les vers doit être synchronisée à une large échelle.

- La communication entre les vers doit être possible, attendu que les réseaux ne sont généralement pas suffisamment segmentés.

---

[39] - Microsoft IIS (5) Unicode/2Xdecode

- Microsoft IIS (4) MSADC

- Microsoft IIS (5) printer extensions

- Microsoft IIS (5) Webdav

- OpenSSL < 0.9.6

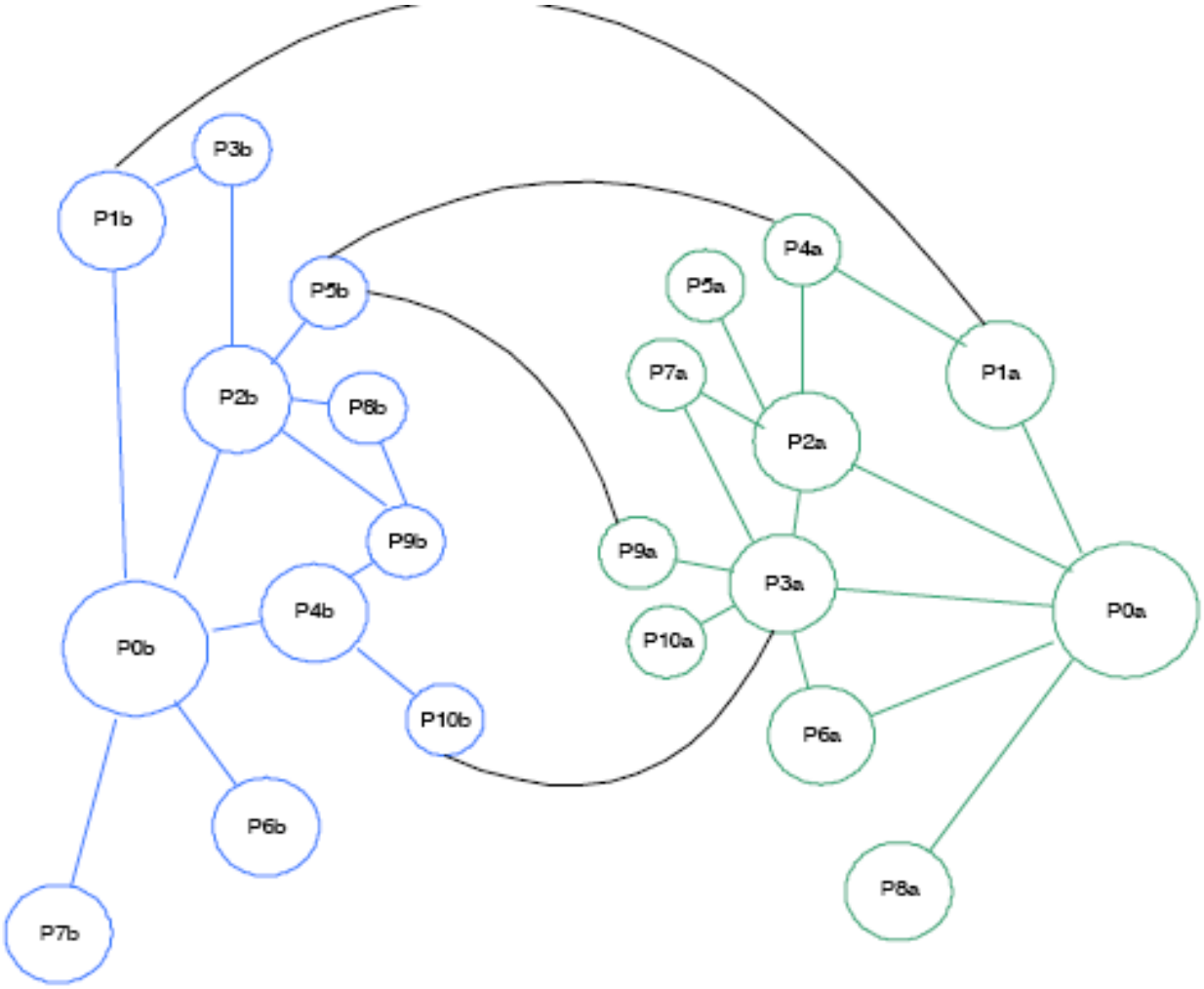
[40] Un réseau local, appelé aussi réseau local d'entreprise (RLE) (ou en anglais LAN, local area network), est un réseau permettant d'interconnecter les ordinateurs d'une entreprise ou d'une organisation. Grâce à ce concept, datant de 1970, les employés d'une entreprise ont à disposition un système permettant : d'échanger des informations, de communiquer et d'avoir accès à des services divers.

- En lancant des fichiers exécutables[41] (.exe), l'infection des machines qui n'ont pas été touchées par les vulnérabilités mentionnées plus avant doit être possible.

2.3.3 La communication entre les vers.

Le défi est, comme nous l'avons vu précédemment, de parvenir à créer un ver qui soit capable de coordination entre ces différentes instances.

Si une instance créait un DoS, même accidentel, elle bloquerait ou ralentirait la dissémination des répliques en d'autres places du réseau, diminuant d'autant l'efficacité du ver et son effet de surprise. L'envoi de messages type "protocole de routage" entre les différentes instances du ver pourrait être la solution.



[41] En informatique, un fichier exécutable est un fichier contenant un programme et identifié par le système d'exploitation en tant que tel. Il existe deux types de programmes exécutables : les scripts textes interprétés par un programme, intégrés directement au système d'exploitation (shells) ou non (perl, php...) et les programmes binaires compilés pour un système spécifique.

Dans le diagramme ci-avant nous considérons que le ver a deux points de départ, nous les nommons patient 0a et patient 0b (P0a et P0b sur le diagramme).

Nous considérons que les vers ne vont pas réinfecter les machines conquises mais qu'au contraire, ils vont se signaler eux-mêmes aux autres instances tentant de les infecter.

On introduit ici un concept de voisinage.

Notre voisin est:

- La machine qui nous a infecté.

- La machine que nous avons infecté.

- La machine avec laquelle vous avez été en contact et qui a déjà été infectée.

Le diagramme ci-avant montre une infection en progression. Le patient 5b a trouvé que les patients 4a et 9a ont déjà été infectés, ils sont alors considérés comme voisin de 5b.

Le patient 3a a comme voisin 10a, 9a(déjà infecté), 0a(il nous a infecté) et 7a, 2a, 6a et 10b (nous l'avons trouvé infecter quand nous nous sommes mis à la recherche de machines encore saines).

Quand une nouvelle infection se produit, la machine à l'origine de l'infection diffuse un message à tous ses voisins afin de se faire connaître des autres instances du ver et être ajouté à la liste "voisinage".

En écoutant les informations diffusées, lors de l'infection, les différentes instances du ver se tiennent informées de l'état du parc informatique. Quand ils ne reçoivent plus d'annonce de contagion pendant une période donnée, on peut considérer que toutes les cibles vulnérables du réseau ont été contaminées. Il est maintenant possible de faire tomber le réseau en lançant l'attaque.

2.3.4 Le déni de service (DoS)

L'attaque par déni de service lancée sur un réseau interne est en général beaucoup plus efficace que son équivalent sur Internet[42].

Il est également possible de rendre le ver plus destructeur en lui ajoutant certaines fonctionnalités. (cf ANNEXE B)

2.3.5 La livraison du ver

Le ver décrit ci-dessus aurait une vie très courte sur Internet car la plupart des vulnérabilités listées plus avant n'existent quasiment pas sur les serveurs frontaux d'Internet. Par contre, les serveurs présents sur les réseaux locaux, naturellement moins exposés, sont plus enclins à présenter des vulnérabilités.

Le défi est de délivrer le ver de telle manière qu'il soit exécuté sur au moins un client présent sur le réseau interne de l'entreprise. Le moyen le plus simple semble être le courrier électronique.

Afin que le ver ne soit pas intercepté par les filtres de contenu mis en place par les administrateurs, il est nécessaire d'utiliser l'encryption SSL[43] ainsi que des techniques d'obscurcissement d'url[44] pour que le destinataire du mail croit qu'il télécharge un fichier présent sur le réseau local. Enfin, on fera en sorte que le courriel semble venir du département informatique de l'entreprise[45].

Afin de tester cette théorie, tous les membres de l'équipe sécurité informatique d'une des plus grosses banques d'Afrique du Sud ont reçu un courriel contenant le ver, ceci sans avoir été informés préalablement.

---

[42] L'avalanche de requêtes étant conditionnée par la vitesse des câbles, on peut atteindre jusqu'à 1 Gigabit/s sur un réseau ethernet contre 0.02Gb/s avec de l'ADSL.

[43] Secure Socket Layer (SSL) est un protocole de sécurisation des échanges sur Internet.

[44] Sigle signifiant uniform resource locator en anglais, littéralement « repère uniforme de ressource ».

[45] On ne peut pas blâmer un utilisateur non-technicien travaillant pour la compagnie xxx de suivre les instructions venant de direction-informatique@xxx.fr et ayant pour objet "nouvel économiseur d'écran, cliquer après le téléchargement" et qui contient un lien vers https://...

Une fois lancé, l'exécutable que l'équipe Sensepost a conçu extrayait le nom d'utilisateur de la variable d'environnement, ouvrait un navigateur invisible et se connectait à un site sous leur contrôle, envoyait une requête vers un fichier html avec le nom d'utilisateur comme paramètre.

Les résultats sont les suivants:

- Le courriel a été envoyé à treize personnes.

- 8 ont téléchargé le fichier .exe (60%).

- 5 ont executé le .exe (38%) et une personne l'a exécuté 3 fois.

Comme le ver est virulent, une seule exécution est nécessaire à sa mise en place. Une fois exécuté, il trouve lui même son chemin vers d'autres machines à infecter.

Si cinq membres de l'équipe de sécurité du secteur financier l'ont exécuté, combien de membres du marketing, des ventes, du back-office ou du management l'auraient fait ?

2.3.6 Une livraison ciblée

Comment trouver les adresses e-mail pour une entreprise cible? Pour ce faire l'équipe de Sensepost a mis en place un logiciel capable d'extraire les adresses de courriel depuis google. Cette méthode n'est plus valide aujourd'hui, mais il est encore possible, grâce à yahoo! d'arriver à des résultats équivalents.

Il suffit simplement de faire une recherche du type +@XYZ.com pour trouver des adresses de cette entreprise.

Prenons par exemple les ministères de l'intérieur et de la défense: (les "xxx" sont ajoutés pour éviter la publicité de ces adresses).

- Une requête de la forme +@interieur.gouv.fr nous permet d'extraire les adresses suivantes: stephane.kowalxxx@interieur.gouv.fr, michel.begxxx@interieur.gouv.fr, thierry.boufxxxx@interieur.gouv.fr etc.

- Une requête vers +@defense.gouv.fr nous donne;

raphael.frexxxx@reserves.terre.defense.gouv.fr, francoise.bilxxxx@defense.gouv.fr, bernard.teyssonnixxx@defense.gouv.fr etc.

L'automatisation du processus peut se réaliser facilement grâce à un script perl[46].

ex: le journal Hurriyet en Turquie possède le domaine hurriyet.com.tr.

$ perl courriels.pl hurriyet.com.tr

$ received 83 hits

L'envoi d'un courrier à 83 employés du journal Hurriyet laisse apparaître une très grande chance de voir un individu télécharger et exécuter l'économiseur d'écran.

2.3.7 Prise d'empreintes par pays

Considérons que le ver ait été développé, que le module chargé d'extraire les adresses de courriel depuis yahoo! est opérationnel et qu'il est également capable d'envoyer le ver aux adresses trouvées.

Pour affecter le plus radicalement le pays cible, il est nécessaire de sélectionner les compagnies et administrations qui sont susceptibles d'être durement touchés par une interruption du réseau informatique et dont le pays est largement dépendant.

Les secteurs suivant viennent rapidement à l'esprit :

- Compagnies de télécommunications (lignes fixes, gsm, satellite) ;

- Fournisseurs d'énergie (hydro-électrique, nucléaire, fossile) ;

- Ministères ;

- Militaires ;

- Médias / journaux en lignes ;

- Services financiers (banque, assurance, bourse) ;

[46] Perl (acronyme de « Practical Extraction and Report Language » ou Langage Pratique d'Extraction et de Rapport) est un langage de programmation créé par Larry Wall en 1987.

- "Business dominant" (secteur d'activité qui dans un pays donné produit une large part du PIB) ;

- Services Médicaux.

2.3.8 L'exploitation

Lors de la réunion Black-Hat 2003, l'équipe de Sensepost a agrémenté son outil d'une interface graphique.

A l'aide d'une mappemonde comportant une projection de l'ensoleillement (On lit moins ses courriels la nuit), on désigne son continent puis on choisit son pays.

Le fait de cliquer sur le pays affiche les domaines des principales compagnies et organisations nationales. Le logiciel offre la possibilité de choisir les secteurs à attaquer :

- Fournisseurs d'énergie ;
- Providers télécoms ;
- Les journaux ;
- L'activité dominante (variable selon les pays) ;
- Les sites gouvernementaux ;
- Les sites militaires ;
- Les services financiers ;

On peut y choisir autant de secteurs souhaités. A l'issue de la sélection, l'utilisateur active l'envoi des courriels contenant le ver ou un lien permettant de le télécharger. Ceci clôt la phase "livraison" du processus et lance l'attaque, entraînant les conséquences que l'on imagine.

La faisabilité d'une attaque massive semble, à la lumière de cet exemple, moins improbable et digne de considération.

3 ENJEUX ET RECOMMANDATIONS

En mai 1999, le General Accounting Office (GAO), a annoncé que ses équipes avaient facilement percé les défenses informatiques protégeant des informations vitales de la NASA. Un pirate pourrait aisément pénétrer le système en utilisant des comptes avec des mots de passe faciles à deviner, voire pas de mot de passe du tout, et détruire l'ensemble des données ou faire perdre le contrôle de certains équipements essentiels. Les représentants de l'agence spatiale ont admis l'existence de beaucoup des " trous " révélés par le rapport du GAO et ont affirmé leur volonté d'améliorer la sécurité de leur dispositif. Ils ont toutefois minimisé l'étendue du problème, en précisant que le GAO n'avait testé qu'un des dix centres de la NASA et qu'il n'était pas possible d'extrapoler ces résultats à l'ensemble. USAT rappelle, non sans ironie, l'investissement d'un milliard de dollars consenti l'an dernier par la NASA pour acquérir de nouveaux systèmes d'information."

3.1 LES ENJEUX

3.1.1 Une frappe étendue : l'exemple Black-Ice

L'exemple suivant est tiré de "Black-Ice, the invisible threat of cyber-terrorism"[47], on y décrit une attaque de grande envergure mariant frappes logiques et physiques. Bien que la probabilité de voir une telle attaque se produire soit très faible, elle a le mérite d'expliquer, à l'aide d'exemples simples, les risques encourus.

L'auteur y présente un groupe de terroristes islamistes prêts à mener une série d'attaques et à se sacrifier pour Allah. La mission a été soigneusement préparée pendant deux ans.

Leur but est de mener une série d'attaques simultanées destinées à causer des dégâts massifs visant les infrastructures électroniques américaines. A travers la destruction d'infrastructures de télécommunications et en portant également atteinte à des vies humaines, les terroristes espèrent générer un vent de panique capable d'influer sur la consommation des ménages ou encore le cours des bourses mondiales.

[47] Dan Verton, McGraw-Hill Companies (août 2003)

La structure est composée d'un chef de 44 ans, Abdul Salah. Il est élégant, calme, et intelligent. Il a émigré d'Arabie Saoudite dans les années 80 et a fini ses études aux Etats-Unis d'Amérique où il a obtenu un haut niveau d'expertise technique en ingénierie.

Son équipe est composée de membres de ce que l'on pourrait appeler la "nouvelle génération" de terroristes : Ils ont décidé d'utiliser les nouvelles technologies pour planifier, coordonner et lancer leurs attaques. Ils porteront des ceintures d'explosifs à la taille. Leur motivation est de heurter l'économie numérique et, à travers elle, l'économie occidentale. Cette "nouvelle génération" de terroristes est constituée de jeunes hommes ayant grandi en occident, intégré le mode de vie local et fréquenté les universités. Ils possèdent des capacités techniques avancées dans différents domaines.

Pour cette nouvelle génération, répandre le sang est insuffisant, les frappes doivent être accompagnées de dysfonctionnements majeurs dans les télécommunications causées par la destruction d'infrastructures sensibles.

Salah a décidé de créer quatre cellules, chacune constituée de cinq opérationnels. Trois d'entre elles sont déjà en place aux Etats-Unis d'Amérique, l'autre arrive du moyen-orient. Les membres ne se connaissent pas.

Salah rencontre en personne les leaders de chaque cellule pour leur donner directement les informations lorsque cela est strictement nécessaire. Le reste du temps, il préfère faire usage d'Internet et échanger des messages chiffrés et dissimulés aux travers d'artifices stéganographiques[48], de boites de courriel restantes, d'obscurs BBS[49] ou de chats privés ponctuels. L'usage du téléphone, jugé trop risqué, est prohibé sauf cas d'urgence.

Les quatre cellules sont constituées d'experts en explosifs, d'électroniciens, d'informaticiens, de personnes capables de collecte et d'analyse d'informations ainsi que d'un chimiste.

---

[48] La stéganographie est l'art de la dissimulation : l'objet de la stéganographie n'est pas de rendre un message inintelligible à autre que qui de droit mais de le faire passer inaperçu. Si on utilise le coffre-fort pour symboliser la cryptographie, la stéganographie revient à enterrer son argent dans son jardin. Bien sûr, l'un n'empêche pas l'autre, on peut enterrer son coffre dans son jardin.

[49] Un BBS (bulletin board system, littéralement : système de bulletins électroniques en français), consiste en un serveur équipé d'un logiciel offrant les services d'échange de messages, de stockage et d'échanges de fichiers, de jeux via un ou plusieurs modems reliés à des lignes téléphoniques.

Salah a un autre atout, un douzaine de pirates informatiques de classe mondiale recrutés en Russie et employés pour mener une série de cyber-attaques contre les réseaux d'ordinateurs qui contrôlent et régulent les infrastructures énergétiques sensibles dans la région où les assauts vont être lancés.

Une fois tous les pions placés, les failles détectées, les exploits préparés et les cibles soigneusement sélectionnées il ne reste plus qu'à lancer l'assaut.

L'attaque a lieu au milieu de l'hiver, ceci afin de stresser le réseau électrique déjà fortement sollicité.

La vague initiale d'attaques consiste en l'explosion de 18 camions de transport de carburant.

La première explosion a lieu au nord de Washington sur l'autoroute 547 à proximité de l'interconnexion de gaz de la région. L'explosion provoque une boule de feu et un épais nuage noir nocif. L'incendie se propage et oblige les autorités à stopper la desserte en gaz des stations électriques de l'état.

Salah reçoit un message chiffré l'avertissant du succès de la première phase.

Les trois attaques suivantes visent des lignes à très haute tension de 500.000 Volts. Les hommes de Salah mettent moins de 60 secondes à couper la chaîne qui leur bloque l'accès au pylône et placent les charges judicieusement.

Dans le même temps, l'équipe de pirates Russe lance son attaque sur les systèmes SCADA, le cerveau numérique des réseaux. Ils attaquent de plusieurs points du globe et injectent vers et virus au coeur du système déjà fortement stressé par les attaques physiques. Les pirates ferment des vannes devant rester ouvertes. Ils lancent ensuite un Déni de Service (DoS) qui paralyse les communications et donc les remontées d'informations des différents organes. Peu de temps après le réseau électrique s'écroule et plonge une partie de la côte Est dans le noir.

Au niveau national, un ver inconnu s'attaque à 10 des 13 Root DNS[50] ralentissant le trafic sur Internet, produisant aussi beaucoup de time-out.

[50] Le Root DNS ou Serveur de Nom de Domaine Racine est le serveur de référence permettant la traduction d'une adresse telle que free.fr en une adresse IP. C'est le principe de l'annuaire téléphonique, du nom on trouve le numéro de la personne que l'on souhaite joindre. Le Root DNS est un maillon essentiel au bon fonctionnement d'Internet.

Les dysfonctionnements s'additionnent et commencent à provoquer des réactions en cascade. On assiste à une avalanche de serveurs.

Les agences gouvernementales qui avaient planifié une telle attaque réagissent bien et mettent en place des parades leur permettant de continuer à travailler. Ce n'est pas le cas de la plupart des entreprises et commerces qui sont paralysés.

A ce stade l'attaque débute.

Au centre de Seattle, un immeuble explose en tuant et blessant des douzaines de personnes. Peu après, dans un appartement au cinquantième étage d'un immeuble une bombe explose. Un des ingénieurs a placé une quantité importante d'explosifs dans un étui en cuivre lui même entouré de fils électrique. Une batterie charge la bobine et crée un électroaimant. Lorsque la bombe explose la bobine produit un court-circuit et compresse les ondes magnétiques, envoyant une impulsion électromagnétique (EMP) similaire à celle d'une explosion nucléaire (sans les destructions physiques). Dans un large rayon, tous les appareils électroniques deviennent inopérants, les communications sont coupées, perturbant les services d'interventions.

Pendant ce temps, d'autres membres de l'organisation sont à bord d'un des camions, ceinture d'explosif autour de la taille, ils sont à plusieurs centaines de miles de Seattle, à San José, la capitale de l'univers numérique. Ils s'arrêtent à proximité de Cesar de Chavez Park, à quelques pas de leur cible. Deux des cinq membres sortent du camion, l'un portant une boite à chaussures, l'autre un pistolet. Le chauffeur du camion fait une embardée et se dirige lentement vers la cible. L'immeuble héberge l'un des noeuds les plus grands et les plus critiques d'Internet, MAE West. Le trentième étage contient un centre névralgique qui connecte la plupart des fournisseurs d'accès. Cet immeuble est le coeur de millions de cession Internet, des milliards de bytes y transitent à chaque seconde.

Le conducteur du camion avance lentement laissant le temps aux deux hommes de pénétrer plus avant dans l'immeuble afin qu'ils disséminent autant d'anthrax que possible.

Le conducteur du camion accélère et fonce vers le building avec ses 40.000 litres de carburant. Les terroristes font détonner leurs bombes et disparaissent avec une grande partie de la façade de l'immeuble. Dans le même temps, le souffle propulse les poussières mêlées d'anthrax vers

les habitations voisines. Ce n'est que quelques jours plus tard que les urgences des hôpitaux commenceront à se remplir de patients se plaignant des syndromes de la grippe et de tâches sombres sur le corps.

Dans les hôpitaux, des patients décèdent de transfusions sanguines avant que l'on constate que les bases de données patient ont été compromises par un virus.

L'attaque sur MAE West a déconnecté certains fournisseurs d'accès Internet de la région, certains sont passés en peering[51], partageant leurs ressources et fonctionnant en mode très dégradé. L'ensemble d'Internet est sévèrement ralenti.

Les coupures d'électricité vont perdurer plusieurs semaines avant que le réseau ne retrouve sa stabilité. Les crashes informatiques en cascade vont se ressentir sur l'ensemble du réseau mondial, perturber les flux financiers, ralentir le commerce en ligne et faire perdre des dizaine de milliards d'euros en manque à gagner. Les effets combinés de la coupure d'électricité et de L'EMP vont couper du monde une partie de la population.

Cet exemple est aujourd'hui de la science-fiction. Toutefois, il repose sur des possibilités réelles. Une telle attaque, menée dans son intégralité parait difficilement réalisable, néanmoins, dans une forme moins étendue elle reste à la portée de quelques groupes internationaux.

3.1.2 L'identification des cyber-terroristes

Il est facile d'obtenir sur Internet une documentation fournie sur les divers modes opératoires visant à compromettre une machine. Il existe des centaines de sites warez qui offrent une multitude d'outils destinés à aider les pirates dans leur tâche.

Il existe également un moteur de recherche, Astalavista, destiné principalement au piratage informatique. Il est possible de trouver, grâce à lui, des informations « légales » concernant le fonctionnement des systèmes informatiques, leur sécurité et leurs vulnérabilités (dans le but

[51] Le Peering est la pratique d'échanger du trafic Internet avec des pairs. Les fournisseurs d'accès Internet (FAIs) configurent des points de peering, les endroits physiques où les échanges de connexions se déroulent et négocient les spécificités du peering. La plupart des points de peering sont situés dans des centres de collocation où les différents opérateurs réseaux centralisent leurs points de présence.

d'y remédier ; ces informations peuvent cependant être utilisées dans le but de nuire, d'où l'ambiguïté du site) mais aussi des numéros de série permettant de débloquer (« cracker ») des programmes en version d'essai, activité considérée comme illégale dans de nombreux pays.

De ce fait l'art est accessible a un grand nombre de personnes. Il ne nécessite pas la manipulation de substances prohibées, la fréquentation de personnes fichées ou le suivi d'un stage en Afghanistan.

L'art du piratage est enseigné dans les écoles d'ingénieurs, les universités, discuté lors de symposiums rassemblant les experts nationaux et internationaux, de la défense, de l'intérieur et du secteur privé.

Quoi qu'il en soit il n'existe à ce jour aucune preuve liant un groupe terroriste à une cyber-attaque massive. Il est difficile de déterminer l'identité des personnes à l'origine des attaques quand, dans le même temps les organisations en charge de la sécurité des systèmes d'information reportent chaque jour d'avantage d'attaques par virus, causant de plus en plus de pertes économiques et affectant des zones géographiques toujours plus étendues.

Selon le CERT américain, le volume des attaques ne cesse d'augmenter : de 132 en 1989, il est passé à 9859 en 1999 et à 137 529 en 2003.

Le volume et la fréquence des attaques rendent difficile la détection des attaques sérieuses et l'identification de leurs auteurs.

3.2 RECOMMANDATIONS

3.2.1 Mise en place d'une structure de réponse rapide

D'année en année, les systèmes de communications étatiques gagnent en importance et en complexité. Si au début des années 90, les communications restaient pour beaucoup analogiques, la tendance s'est rapidement inversée, au point de conditionner la bonne marche de l'économie. On considère qu'une interruption d'Internet pendant une journée sur l'ensemble du territoire national aurait un impact visible sur le PIB annuel.

Aujourd'hui, les systèmes de communications français pourraient subir une attaque venant du cyber espace. Il est donc nécessaire de mettre en place un système de veille capable de

détecter les activités suspectes susceptibles de porter atteinte à nos infrastructures, d'analyser les "exploits", d'alerter les victimes potentielles afin d'organiser une réponse rapide et de restaurer les services endommagés.

La difficulté de cette tâche est grande, en particulier parce qu'il n'existe aucun point d'observation panoramique avantageux duquel il serait possible de voir l'origine des attaques et leur propagation.

Pour limiter l'impact d'une cyber-attaque, il est nécessaire de diffuser les informations la concernant de manière rapide et étendue. Les organismes de prévention et de lutte peuvent exister dans nombre d'infrastructures publiques ou privées. Elles doivent être coordonnées pour réagir efficacement contre une attaque, en limiter les effets et rétablir les systèmes endommagés.

L'un des éléments essentiels de réussite de cette équipe de "réaction rapide" devra être sa capacité de communication et d'initiative. Elle se traduira par un formalisme allégé des échanges entre les partenaires gouvernementaux mais aussi non-gouvernementaux. Le souci sera ici l'efficacité et l'inter-activité.

Il est évident que cette équipe devra également communiquer avec les partenaires communautaires afin d'apporter une réponse globale à la menace, en publiant des alertes, ainsi que des avis sur les mesures à mettre en place.

Constatant que le secteur privé fait l'objet de la majorité des attaques, il sera souvent le premier à les détecter, l'instituant de fait en partenaire privilégié.

Le fonctionnement de l'équipe de réponse rapide devra répondre à un schéma simple, comprenant quatre secteurs, à savoir l'analyse, l'alerte, la gestion de crise et la réponse.

- L'analyse est la première étape du cheminement qui va mener à une compréhension aussi fine que possible des types d'attaques, de leurs origines et de leurs degrés de dangerosité. Elle permet aussi de connaître la nature des dommages, l'étendue de la compromission et d'évaluer les moyens à mettre en place pour y faire face. Elle peut aussi fournir des informations sur les intentions de l'attaquant, les outils utilisés et les vulnérabilités qu'il a exploitées.

- L'alerte, quant à elle, est contingente à la capacité de détection de cette équipe. L'absence d'une vue synoptique d'Internet complique considérablement la tâche des veilleurs. Il est donc nécessaire de se rapprocher à la fois des CERTs mais aussi des acteurs privés.

Les effets d'une attaque sur un secteur peuvent, par effets domino, affecter plusieurs autres secteurs et rapidement dépasser les compétences et capacités de structures privées ou régionales.

Dans le même esprit, l'industrie devrait être encouragée à développer un mécanisme permettant le partage de l'information sur la "santé" d'Internet afin d'améliorer l'analyse, les alertes, les réponses et la sortie de crise. Ce genre de coopération volontaire, établie dans le respect des lois et règlements, permettrait un partage pertinent d'information entre les fournisseurs d'accès Internet[52] (FAI) et autres acteurs majeurs du réseau capable d'affiner l'analyse. Ce type de coopération permettrait d'éviter que l'utilisation massive de certains exploits causant d'importants dommages voire une interruption de systèmes névralgiques.

Une bonne gestion du temps peut faire la différence entre une interruption majeure et un incident mineur. Améliorer les capacités nationales d'alerte nécessite une infrastructure sécurisée capable d'assurer le bon acheminement des communications entre les différents acteurs étatiques ou privés, malgré un dysfonctionnement majeur d'Internet. Ce réseau privé doit pouvoir supporter des conférences (voix) et des échanges de fichiers.

- La gestion de crise doit se faire en partenariat avec les agences nationales et les ministères concernés. On peut, à titre d'exemple, citer la Défense, l'Intérieur, la Justice, l'Industrie, les Finances et la Recherche.

Pour qu'une réponse rapide et efficace soit mise en place, deux mesures préalables doivent être prises.

- La mise en place d'un processus de développement de partenariat public-privé ainsi que la création de procédures d'urgences répondant à différents scénarii.

[52] un FAI, est un organisme (généralement une entreprise) offrant une connexion au réseau informatique Internet à des particuliers et à des entreprises. Le terme anglais désignant un FAI est Internet service provider, abrégé ISP.

- L'établissement de procédures d'urgences est un élément clef de la réussite, aussi bien face au terrorisme classique qu'au cyber-terrorisme. En l'absence de procédure d'urgence et d'exercice, les différentes directions concernées pourraient ne pas pouvoir faire face à une interruption massive des communications via Internet.

L'intérêt des exercices réside, outre dans le fait de développer des automatismes, à découvrir des faiblesses diminuant d'autant la vulnérabilité des infrastructures.

3.2.2 Programme de réduction des menaces et vulnérabilités

Si les acteurs de la menace sur Internet sont très divers ils cherchent tous à exploiter les mêmes faiblesses, qu'elles viennent du protocole IPv4[53], des erreurs structurelles du réseau, du hardware, ou des logiciels.

Il n'est pas judicieux ni prudent d'attendre qu'une information sur la survenue prochaine d'une attaque nous parvienne avant d'agir. Parce que ce genre d'information est rarement connu avant le début de l'attaque mais aussi parce que la connaissance de l'attaque et de la vulnérabilité qu'elle exploite n'assure en rien que nous serons capables d'y faire face dans un délai raisonnable. Il arrive parfois qu'il s'écoule des jours voire des semaines avant qu'une parade puisse être découverte et qu'un correctif soit mis à disposition des utilisateurs.

L'évolution rapide des logiciels et des systèmes d'exploitation, toujours plus complexes, écarte catégoriquement l'hypothèse d'un parc informatique déchargé de toute faille.

Pour preuve, le 21 juillet 2005, soit quelques jours après la sortie de la version beta de Windows Vista™ Microsoft© faisait face à un premier virus[54]. Celui-ci, nommé "second part to hell", exploite une faille de sécurité du nouveau shell[55] de Microsoft nommé monad.

---

[53] Le protocole IP fait partie de la couche Internet de la suite de protocoles TCP/IP. C'est un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport des datagrammes IP (les paquets de données), sans toutefois en assurer la « livraison ». En réalité, le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition

[54] Windows Vista: premier virus identifié!

<http://www.generation-nt.com/actualites/8477/Windows-Vista-premier-virus-identifie>

[55] L'interpréteur de commandes est l'interface entre l'utilisateur et le système d'exploitation, d'où son nom anglais «shell», qui signifie «coquille». Le shell est ainsi chargé de faire l'intermédiaire entre le système d'exploitation et l'utilisateur grâce aux lignes de commandes saisies par ce dernier. Son rôle consiste à lire la ligne de commande, interpréter sa signification, exécuter la commande, puis retourner le résultat sur les sorties.

L'apparition de ce virus peut inquiéter quand on sait que Microsoft© a mis l'accent sur la sécurité et que la sortie de Windows Vista™ est prévue fin 2007.

La nature "anationale" du réseau Internet en fait un terrain de jeu privilégié pour les pirates et criminels qui y voient une opportunité de perpétrer des méfaits sans être poursuivis. Les magistrats, de leur côté, peinent à comprendre les subtilités de l'informatique et se heurtent à des concepts qui dépassent leur compréhension. L'arsenal juridique est quant à lui mal adapté et trouve sa limite le plus souvent aux frontières nationales.

Les activités illicites sur le réseau, le spam[56], la propagation de vers ou virus, érodent la confiance des utilisateurs et heurtent l'économie ou notre sécurité au travers des attaques contre nos infrastructures.

C'est donc idéalement en se donnant la capacité de poursuite des attaquants, par des investigations, des arrestations, des inculpations puis des condamnations qu'il sera possible d'atténuer l'engouement des pirates. Ceci fait, les agences concernées pourront se concentrer sur les menaces les plus sérieuses sans être polluées par une nuée de script-kiddies[57] gonflés d'un sentiment d'impunité.

Pour les affaires les plus sérieuses, les autorités judiciaires trouveront, dans la diplomatie, un allié de premier ordre.

Enfin, les efforts des différents services et les fruits de leurs investigations devront, sauf nécessités exprimées par les autorités, être largement diffusées auprès des entreprises et administrations afin d'améliorer la sécurité globale des infrastructures.

---

[56] Le spam, mot anglais du jargon informatique, désigne les communications électroniques massives, notamment de courrier électronique, sans sollicitation des destinataires, à des fins publicitaires ou malhonnêtes.

[57] Ce terme désigne les pirates informatique néophytes qui, dépourvu des principales compétences en matière de gestion de la sécurité informatique, passent l'essentiel de leur temps à essayer d'infiltrer des systèmes, en utilisant des scripts ou autres programmes mis au point par d'autres crackers.

Malgré leur faible niveau de qualifications, les script-kiddies sont parfois une menace réelle pour la sécurité des systèmes car d'une part ils sont très nombreux et d'autre part ils sont souvent obstinés au point de passer parfois plusieurs jours à essayer toutes les combinaisons possibles d'un mot de passe, avec le risque d'y parvenir.

Les informations collectées, ainsi que le savoir faire associé peuvent également être utilisés pour examiner la robustesse de nos infrastructures et les capacités de détections et de réactions des organismes ciblés.

En résumé, il est nécessaire de chercher à prévenir, décourager, et réduire de manière significative les cyber-attaques en assurant l'identification et la poursuite des délinquants. Dans le cas de cyber-crimes, la réponse doit être rapide et quasi certaine, la punition, quant à elle, doit être suffisamment sévère pour être dissuasive.

CONCLUSION

Le cyber-terrorisme n'existe pas stricto sensu à ce jour. Les avis des experts diffèrent, les uns pensant que jamais une attaque opérée depuis le cyber espace ne pourra entraîner de pertes humaines, les autres considérant que le monde n'est peut être pas encore mûr pour ce genre d'attaque mais que dans un avenir sans doute peu lointain nous devrons y faire face.

Comme nous l'avons constaté, les attaques menées depuis Internet demandent des budgets relativement faibles alors qu'elles peuvent produire des effets importants. Ainsi certains pays ont décidé de développer leurs capacités dans ce domaine en espérant compenser les faiblesses de leur arsenal militaire.

Un autre côté attractif est le faible risque inhérent à ce type d'attaque. Internet est encore aujourd'hui un vaste royaume où l'impunité règne, les moyens offerts aux forces de l'ordre ainsi que le manque de coopération internationale rendent les arrestations difficiles, voire impossibles.

Si Internet présente un intérêt pour les terroristes, du point de vue de la propagande (au travers de la diffusion de revendications, de vidéos d'exécutions), il entraîne des effets moins spectaculaires qu'une attaque cinétique visant le métro ou les aéronefs.

Toutefois, le terrorisme évolue, les plus radicaux sont souvent de jeunes convertis qui ne parlent pas ou peu l'arabe mais qui ont reçu une bonne éducation et sont capables de se fondre dans la population sans attirer l'attention des autorités. Cette nouvelle génération de terroristes de plus en plus rompue aux secrets de l'informatique, pourrait dans quelques années, devenir une véritable préoccupation pour les services de l'Etat.

Les systèmes d'exploitation sont de plus en plus complexes et de ce fait comportent un nombre croissant d'erreurs de programmation permettant une prise de contrôle à distance. Les efforts des éditeurs de logiciels ne donnent pas beaucoup de résultats et il est à craindre que le nombre d'attaques continue de progresser, comme c'est le cas depuis la fin des années 80. Par ailleurs, les utilisateurs, peu conscients des risques encourus ne font pas suffisamment preuve de prudence et fournissent de ce fait des armes aux pirates informatiques.

A la lumière de ces réflexions, il est raisonnable de penser que la menace cyber-terroriste, si elle se dessine à l'horizon, n'est pas encore clairement visible. Néanmoins, même si la

probabilité d'une attaque est faible, le risque est pris en compte par nombre d'états et suscite la discussion parmi les experts. La prise en compte de la menace cyber-terroriste doit comporter deux grands axes : la lutte contre la cyber-criminalité (connaissance des acteurs et des outils) et la lutte contre le terrorisme classique (connaissance des milieux et tendances). Elle doit également passer par la mise en place de plans de prévention visant à réduire l'impact d'une hypothétique attaque.

Pour l'heure, autant on peut attester de l'utilisation d'Internet par des terroristes (propagande, financement, formation), autant rien de permet d'attester qu'une véritable attaque cyber-terroriste ait jamais abouti.

ANNEXES

A - Rapport Calipari (extrait)

4. (U) Communications Regarding the Mission Duration

(U) Captain Drew, Second Lieutenant Acosta, and Staff Sergeant Brown were all concerned about the length of time that the Soldiers had been manning their blocking positions. (Annexes 74C, 77C, 83C). Captain Drew was concerned that leaving his Soldiers in a static position for more than 15 minutes left them open to attack. He was also concerned that he was not adequately performing his patrolling mission because his Soldiers were tied down to the blocking positions. (Annex 74C).

(U) Captain Drew checked with the 1-69 IN TOC at least two times seeking to collapse the blocking positions and return his Soldiers to their patrolling mission. The 1- 69 IN TOC, after checking with 2/10 MTN TOC, informed him that the convoy had not passed and to stay in position. (Annexes 74C, 2L).

(U) At 2010 hours, the 2/10 MTN Battle Captain requested permission from the 3ID TOC to remove blocking positions until 15 minutes before VIP movement. (Annex 2L).

(U) At 2014 hours, the 3ID TOC Battle Captain informed the 2/10 MTN Battle Captain that A Company, 1-69 IN could reduce their blocking positions until 2018 hours. (Annex 2L).

(U) At 2015 hours, the 2/10 MTN Battle Captain reported to the 3ID TOC Battle Captain that A Company, 1-69 IN blocking positions would remain in place. (Annex 2L).

(U) At 2020 hours, the 2/10 MTN Battle Captain notified 1-69 IN to keep blocking

positions in place. (Annex 2L).

(U) At 2030 hours, Captain Drew asked again about collapsing the blocking positions.

He was told that the word from 3ID was not to move off the blocking positions, that the convoy would be coming down Route Irish in approximately 20 minutes, and that the convoy would consist of four HMMWVs and an up-armored Suburban. (Annexes 97C, 3L).

(S//NF) 1-76 FA was able to communicate the requirement for blocking positions along Route Irish for a VIP movement from the International Zone to BIAP. (Annexes 58C, 59C, 62C, 63C). The security escort platoon with the VIP was able to, and did, relay departure and arrival times to the 1-76 FA Battle Captain. (Annexes 59C, 64C).

The VIP convoy departed the International Zone in four HMMWVs (and no Suburban) at approximately 1945 hours. It arrived at the Camp Victory gate at 2010 hours (Annex 59C). The convoy reached its destination on Camp Victory at 2020 hours (Annex 59C). The VIP returned to the International Zone by helicopter at approximately 2205 hours. The determination to fly by helicopter back to the International Zone was not made until shortly before the VIP departed as a result of clearing weather conditions. (Annexes 59C, 64C).

(S//NF) The 1-76 TOC had two means of communicating with 4th Brigade, its higher headquarters: Voice Over Internet Protocol (VOIP)2 and FM. **The 1-76 FA Battle Captain was using only VOIP to communicate with 1-69 IN, but experienced problems with VOIP, therefore losing its only communication link with 1-69 IN**, other than going through 4th Brigade. (Annex 97C). As a result, the Battle Captain was unable to pass updated information about the blocking mission either directly to 1-69 IN, or to 4th Brigade. He did not attempt to contact 4th Brigade via FM communications. (Annex 63C). Fourth Brigade, in turn, could not pass updated information to its major command, 3ID. (Annex 57C). Likewise, 3ID had no new information to pass to its subordinate command, 2/10 MTN. Finally, 2/10 MTN was thus unable to pass updated information to its subordinate command, 1-69 IN. (Annexes 51C, 52C).

(U) There is no evidence to indicate that 1-76 FA passed on the information about the VIP departure and arrival times to any unit. (Annexes 59C, 63C). **As a result, A Company, 1-69 IN's Soldiers were directed to remain in their blocking positions.**

E. (U) The Incident

(U) After arriving at BIAP from Italy in the late afternoon of 4 March 2005, and taking care of some administrative matters, Mr. Carpani and Mr. Calipari went to some undisclosed location in the Mansour District of Baghdad. (Annexes 104C, 105C). At approximately 2030

hours they recovered Ms. Sgrena and headed back toward BIAP. (Annexes 103C, 104C, 109C). Both agents made a number of phone calls to various officials during the drive. (Annex 104C). Mr. Carpani was mostly talking to his colleague, Mr. Castilletti, who was waiting for them outside of BIAP near Checkpoint 539. He updated Mr. Castilletti on his location and discussed arrangements at the airport. (Annex 105C). Mr. Carpani, who was driving, had to slow down at one point due to a flooded underpass on Route Vernon. (Annexes 103C, 104C). Mr. Carpani, who had experience driving in Baghdad, did not have an alternate route to the airport planned.

(S//NF) VOIP is a technology that allows telephone calls to be made using a broadband Internet connection instead of a regular (analog) phone line.

CLASSIFIED

B - Un ver plus destructeur

- Injection de 10 bits de manière aléatoire dans tous les fichiers de Microsoft© Office, les fichiers compressés .zip, les bases de données peuvent également être touchées.

- Changer les paramètres du BIOS[58], y ajouter un mot de passe, ou flasher[59] le BIOS avec un logiciel défectueux, ce qui interdira tout redémarrage de l'ordinateur et obligera à un retour usine.

- Afficher une fenêtre invitant l'utilisateur à contacter d'urgence l'administrateur;

" vous devez contacter votre administrateur et lui fournir les caractères suivants afin qu'il réactive votre accès; aiUBGncPP6xFYcdGOaxezPJ5 "

Ce message vise à saturer le bureau informatique d'appels téléphoniques, perturbant le personnel et l'empêchant de passer des appels à ses collègues alors qu'il doit faire face à un vrai problème.

- Déterminer si les routeurs[60], switchs et hubs sont configurés avec les mots de passe par défaut. Si c'est le cas, changer les mots de passe d'administrateur. La recherche se fait sur les "login/mot de passe" configurés en sortie d'usine. Il est préférable de se concentrer sur les acteurs majeurs du secteur à savoir Cisco et 3Com. Le changement de mot de passe empêchera les administrateurs de contenir à distance l'infection.

---

[58] Le Basic Input Output System ou BIOS (système de base d'entrée/sortie) est un programme contenu dans la mémoire morte (ROM) de la carte mère s'exécutant au démarrage de l'ordinateur. Il déclare les disques, configure les composants et recherche un système d'exploitation avant de le lancer. Sa tâche principale est de fournir un support de bas niveau pour communiquer avec les périphériques.

[59] Il existe désormais des cartes-mères comportant des mémoires flash, mémoires pouvant être modifiées directement par logiciel. Les BIOS situés sur des cartes-mères comportant ce type de mémoire peuvent être mis à jour (le terme « upgrader » est parfois utilisé, mot francisé provenant du verbe to upgrade qui signifie mettre à jour) grâce à un programme appelé firmware, fourni par le fabricant, destiné à permettre le remplacement de l'ancien BIOS par un BIOS plus récent. Le problème consiste toutefois à se procurer les mises à jour de son BIOS (problème maintenant résolu grâce à l'accès à Internet). Ces mises à jour sont disponibles sous forme de fichier binaire contenant une image du BIOS, et qui sera transférée dans la mémoire flash grâce au firmware.

[60] Un switch ou commutateur est un dispositif électronique servant de commutateur réseau et permettant de créer un réseau informatique local de type ethernet. Ce dispositif est dit intelligent par opposition au hub car, alors que ce dernier fait transiter les données par toutes les machines, le switch permet de diriger les données uniquement vers la machine destinataire.

Il existe quatre moyens pour le ver de trouver les bornes du réseau:

- Obtenir l'adresse IP et le masque de la machine cible. Une machine avec plusieurs interfaces réseaux est un bonus

- Envoyer des requêtes SNMP[61] utilisant des chaînes de caractères communes pour en extraire les tables de routage.

- Faire un traceroute[62] sur les adresses IP localisées sur les machines connues dans le but d'enregistrer les chemins.

- Faire des ping[63] sur les adresses IP des réseaux de classe C au dessus et en dessous du réseau actuel.

ex: si le réseau est 10.0.10.0/24 essayer 10.0.9.0/24 et 10.0.11.0/24

[61] Le sigle SNMP signifie Simple Network Management Protocol (protocole simple de gestion de réseau en Français). Il s'agit d'un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau et de diagnostiquer les problèmes de réseau.

[62] Traceroute est un outil réseau qui permet de suivre le chemin qu'un paquet de données (paquet TCP ou UDP) va prendre pour aller d'une machine A à une machine B.

[63] Ping est le nom d'une commande (développée par Mike Muuss) permettant d'envoyer une requête ICMP à une autre machine. Si la machine ne répond pas il se peut que l'on ne puisse pas communiquer avec cette machine.

Bibliographie

The Next War Zone: Confronting the Global Threat of Cyberterrorism
de James F. Dunnigan
Citadel Press (septembre 2003)

Black Ice: The Invisible Threat of Cyber-Terrorism
de Dan Verton
McGraw-Hill Companies (août 2003)

Computer Attack and Cyber Terrorism:
Vulnerabilities and Policy Issues for Congress
de Clay Wilson,
The Library of Congress (2005)

Federal Intrusion Detection, Cyber Early Warning and the Federal Response
Brian Fuller,
Sans Institute (2003)

Can Cyber Terrorists Actually Kill People?
Scott Anthony Newton,
Sans Institute (2002)

Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure
Shannon M. Lawson,
Sans Institute (2003)

Redefining the Role of Information Warfare in Chinese Strategy
Edward Sobiesk
Sans Institute (2003)

Annual Report on the Military Power of the People!s Republic of China.
Report to Congress (28 Juillet 2003)

Internet et Sécurité
de Solange Ghernaouti-Helie, Arnaud Dufour, Que sais-je?
Presses Universitaires de France - PUF (15 juin 2002)

La Violence et la Paix
de Pierre Hassner
Seuil (3 mars 2000)

La Terreur et l'Empire : La Violence et la Paix, tome 2
de Pierre Hassner
Seuil (5 septembre 2003)

Question(s) d'Intelligence : Le Renseignement Face au Terrorisme
de Bruno Delamotte
Editions Michalon (28 mai 2004)

Techniques du Terrorisme
de Jean-Luc Marret
Presses Universitaires de France - PUF (18 mars 2002)

The 9/11 Commission Report

The Future of Cyber Terrorism:
Where the Physical and Virtual Worlds Converge
Barry C. Collin
Institute for Security and Intelligence

Managerial Guide For Handling Cyber-terrorism And Information Warfare
de Lech Janczewski
Idea Group Publishing (avril 2005)

Cyber Terrorism: A Guide for Facility Managers
de Joseph Gustin
Marcel Dekker (octobre 2003)

The Myth of Cyber Terrorism
De Joshua Green
http://www.washingtonmonthly.com/features/2001/0211.green.html

Hypothecising the Cyber Terrorism
Brett Kraynak
George Washington University (2002)

Cyber-Terrorism - Fact or Fancy?
Mark M. Pollitt
FBI Laboratory

Cyber Terrorism, Testimony before the Special Oversight Panel on Terrorism Committee
Dorothy E. Denning
Georgetown University (23 Mai 2000)

The National Strategy To Secure Cyberspace
The White House 2003